Industrial Ethernet managed Switches

Manual

for

Weidmüller managed switches

of series

ValueLine and PremiumLine

First Edition, June 2014

1536330000/00/06.14

Weidmüller

Industrial Ethernet managed Switches Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright ©2014 Weidmüller Interface GmbH & Co. KG
All rights reserved.
Reproduction without permission is prohibited.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Weidmüller.

Weidmüller provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Weidmüller reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Weidmüller assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Contact Information

Weidmüller Interface GmbH & Co. KG
Postfach 3030
32760 Detmold
Klingenbergstraße 16
32758 Detmold
Germany

Phone +49 (0) 5231 14-0
Fax +49 (0) 5231 14-2083
E-Mail info@weidmueller.com
Internet www.weidmueller.com

Table of Contents

1. About this Manual 5

2. Getting Started 6

2.1 Serial Console Configuration (115200, None, 8, 1, VT100) 7

2.2 Configuration by Telnet Console 9

2.3 Accessing configuration interface via Web Browser 11

2.3.1 Accessing the Webinterface via HTTP 11

2.3.2 Accessing the Webinterface via HTTPS 13

2.4 Accessing configuration interface via SSL 14

2.5 Disabling Telnet and Browser Access 15

3. Featured Functions 16

3.1 Configuring Basic Settings 17

3.1.1 System Identification 17

3.1.2 Password 18

3.1.3 Accessible IP List 19

3.1.4 Port Settings 20

3.1.5 Network Parameters 22

3.1.6 GARP Timer Parameters 25

3.1.7 Time 26

3.1.7.1 System Time Settings 26

3.1.7.2 IEEE 1588 PTP 28

3.1.8 Turbo Ring DIP Switch (Menu item and DIP switches) 32

3.1.9 System File Update (Firmware and Configuration) 34

3.1.9.1 Update System Files by Remote TFTP 34

3.1.9.2 Update System Files by Local Import/Export 35

3.1.9.3 System File Update by EBR-Module 36

3.1.10 Security 37

3.1.10.1 User Login Authentication 37

3.1.10.2 Using Port Access Control 39

3.1.11 Restart 46

3.1.12 Factory Default 46

3.1.13 Loop Protection 46

3.2 Using Port Trunking 47

3.2.1 Port Trunking Settings 48

3.3 Configuring SNMP 50

3.3.1 SNMP Read/Write Settings 51

3.3.2 Trap Settings 53

3.3.3 Private MIB Information 54

3.4 Using PoE (PoE Models Only) 55

3.4.1 PoE Settings 55
3.4.2 PoE Timetabling 57
3.4.3 PoE Status 57
3.4.4 PoE Email Warning Events Settings 58
3.4.5 PoE Relay Warning Events Settings 58
3.5 Communication redundancy 59
3.5.1 Introduction to Communication Redundancy 59
3.5.2 The Turbo Ring Concept 60
3.5.2.1 Topology Setup for “Turbo Ring (V1)” or “Turbo Ring V2” 60
3.5.2.2 Ring Coupling Configuration 62
3.5.2.3 Dual-Ring Configuration (applies only to “Turbo Ring V2”) 63
3.5.2.4 Dual-Homing Configuration (applies only to “Turbo Ring V2”) 63
3.5.3 Configuring “Turbo Ring (V1)” and “Turbo Ring V2” 64
3.5.3.1 Configuring Turbo Ring (V1, original version) 64
3.5.3.2 Configuring Turbo Ring V2 (new version) 66
3.5.4 The Turbo Chain Concept 70
3.5.5 Configuring “Turbo Chain” 70
3.5.5.1 Head Switch Configuration 71
3.5.5.2 Member Switch Configuration 71
3.5.5.3 Tail Switch Configuration 71
3.5.6 STP / RSTP 73
3.5.6.1 The STP / RSTP Concept 73
3.5.6.2 How STP Works 75
3.5.7 Configuring STP / RSTP 78
3.6 Using Traffic Prioritization 81
3.6.1 The Traffic Prioritization Concept 81
3.6.2 Configuring Traffic Prioritization 84
3.6.2.1 QoS Classification 84
3.6.2.2 CoS Mapping 87
3.6.2.3 ToS/DiffServ Mapping 88
3.7 Using Virtual LAN 88
3.7.1 The Virtual LAN (VLAN) Concept 88
3.7.2 Configuring Virtual LAN 92
3.7.2.1 VLAN Settings 92
3.7.2.2 Port-Based VLAN Settings 94
3.7.2.3 VLAN Table 95
3.8 Using Multicast Filtering 96
3.8.1 The Concept of Multicast Filtering 96
3.8.2 Configuring IGMP Snooping 99
3.8.3 IGMP Table 101
3.8.4 Static Multicast MAC Addresses 102
3.8.5 Configuring GMRP 103
3.8.6 GMRP Table 103
3.9 Using Bandwidth Management 104

3.9.1 Configuring Bandwidth Management 104
3.9.2 Traffic Rate Limiting Settings 107
3.10 Using Auto Warning 108
3.10.1 Configuring Email Warning 108
3.10.2 Event Types 109
3.10.3 Email Settings 110
3.10.4 Configuring Relay Warnings 112
3.11 Line-Swap-Fast-Recovery 114
3.11.1 Configuring Line-Swap Fast Recovery 114
3.12 Set Device IP 114
3.12.1 Configuring Set Device IP 115
3.12.2 DHCP Relay Agent (Option 82) 116
3.13 Using Diagnosis 119
3.13.1 Mirror Port 119
3.13.2 Ping 120
3.13.3 LLDP Function 120
3.13.3.1 Overview 120
3.13.3.2 Configuring LLDP Settings 121
3.14 Using Monitor 122
3.14.1 Monitor by Switch 122
3.14.2 Monitor by Port 122
3.14.3 Monitor by SFP 123
3.15 Using the MAC Address Table 124
3.16 System Log 125
3.16.1 Using Event Log 125
3.16.2 Syslog Settings 126
4. Using Industrial Protocols 127
4.1 MODBUS/TCP MAP 127
4.2 Profinet I/O 134
4.2.1 PROFINET Environmental Introductions 134
4.2.2 Configuring PROFINET I/O on Weidmüller Switches 135
4.2.3 Step 7 Integration 136
4.2.4 Overview of Operation Procedure 137
4.2.5 Create a PROFINET I/O Subnet Project 137
4.2.6 GSD File Installation 140
4.2.7 Device Configuration 142
4.2.8 Configuring device properties 145
4.2.9 Download the Project into the PLC 146
4.2.10 Monitoring the Switch 147
4.2.11 I/O Device Diagnostics 150
4.2.12 Topology Editor 151
4.2.13 PROFINET I/O Parameters 153

A. Weidmüller Switch Configuration Utility 156

A1.1 Starting Weidmüller Switch Configuration Utility 157
A1.2 Broadcast Search 157
A1.3 Search by IP Address 158
A1.4 Unlock the Ethernet Switch 159
A1.5 Upgrade Firmware 160
A1.6 Modify IP Address 161
A1.7 Export Configuration 162
A1.8 Import Configuration 163

B. MIB Groups 165

B1.1 Supported standard MIB II groups 165
B1.2 Implemented SNMP Traps 166

C. Download links (Software and Documentation) 167

1. About this Manual

Thank you for purchasing a Weidmüller managed Industrial Ethernet switch. Read this user's manual to learn how to connect your Weidmüller switch to Ethernet-enabled devices used for industrial applications.

The following chapters are covered in this user manual:

☐ **Getting Started**

This chapter explains how to connect to the Weidmüller Switch for configuration. There are three ways to access the Switch's configuration settings:

- Serial console
- Telnet console and
- Web console

☐ **Featured Functions**

This chapter explains how to access the Switch's various configuration, monitoring, and administration functions. These functions can be accessed by serial, Telnet, or Web console. The Web console is the most user-friendly way for configuring and monitoring. In this chapter, we use the Web console interface to introduce the functions.

☐ **Communication Redundancy**

This chapter explains how to use the various implemented redundancy features

- Turbo Ring (original version V1) and Turbo Ring V2
- Turbo Chain
- STP/RSTP

☐ **Industrial Protocol Guide**

This chapter explains how to use the Switch the implemented industrial automation protocols

- Profinet
- Modbus TCP

☐ **Weidmüller Switch Configuration Utility**

This chapter explains how to use external PC-tool **Switch Configuration Utility** which is very helpful

- to detect Weidmüller switches which are attached to the same LAN as the PC host (regardless of whether or not you know the IP addresses of the switches)
- to connect to an Weidmüller switch whose IP address is known
- to modify the network configurations of one or multiple Weidmüller switches
- and to update the firmware of one or more Weidmüller Switches.

2. Getting Started

In this chapter we explain how to install a Weidmüller switch for the first time. There are three ways to access the Weidmüller switch's configuration settings: serial console, Telnet console, or web console. If you do not know the Weidmüller switch's IP address, you can open the serial console by connecting the Weidmüller switch to a PC's COM port with a short serial cable. You can open the Telnet or web console over an Ethernet LAN or over the Internet.

The following topics are covered in this chapter:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Configuration by Telnet Console**
- **Configuration by Web Browser**
- **Disabling Telnet and Web Browser Access**

2.1 Serial Console Configuration (115200, None, 8, 1, VT100)

Note about simultaneously connections

You **cannot connect** to the Ethernet Switch simultaneously by serial console and Telnet.

You **can connect** to the Ethernet Switch simultaneously by web browser and serial console or by web browser and Telnet. However, we strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your Ethernet Switch.

Useful tools for serial communiction

Windows XP: We recommend using Hyper Terminal Program, which is installed under Windows XP operating system.

Windows 7: Unfortunately the Hyper Terminal Program is no longer available in Windows 7. Either use a commercial tool for serial communication or alternatively you can use a freeware tool like **PuTTY** or **ucon**.

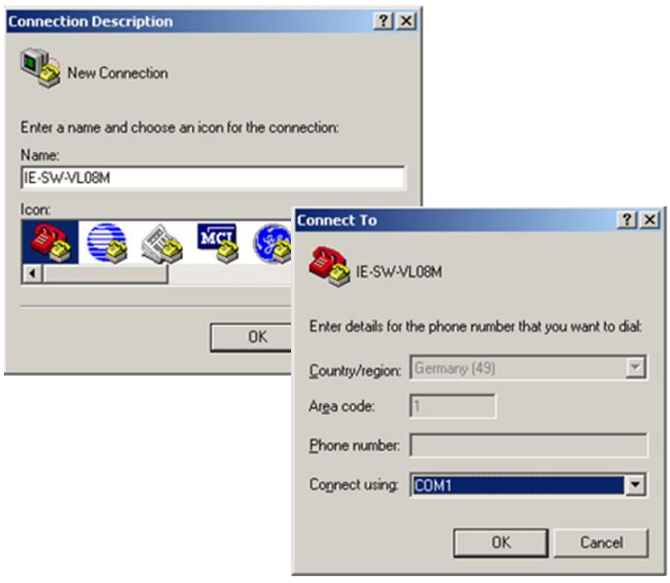
Example of serial connection via Hyper Terminal

Before running Hyper Terminal Program, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect to the Ethernet Switch's RS-232 Console port to your PC's COM port.

After starting Hyper Terminal Program perform the following steps to access the RS-232 Console utility.

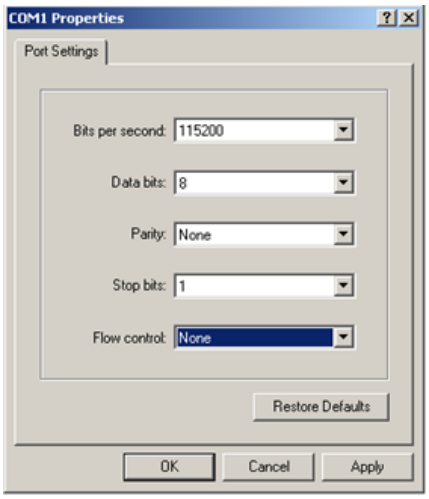
From the Windows desktop, click **Start → Programs → Accessories → Communications → Hyper Terminal.**

Start Hyper Terminal and enter a name of your choice for the new connection. Select the appropriate COM port for console connection in the "New Connection" window.

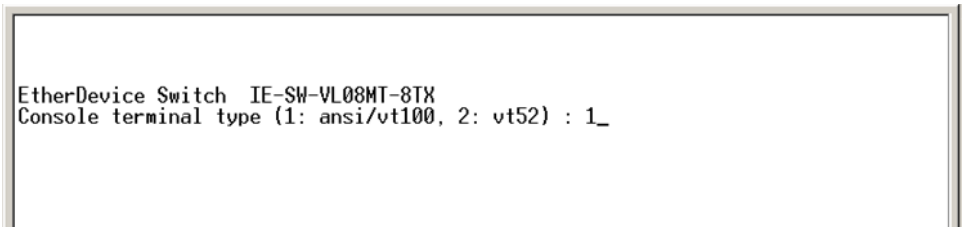


The **Communication Parameter** for console connection are:

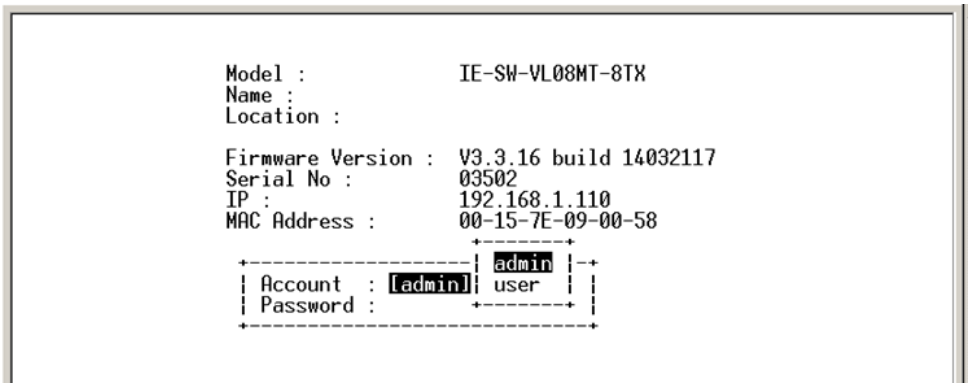
115200 for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, **1** for **Stop Bits,** and **None** for **Flow control**. Click **OK** to continue.



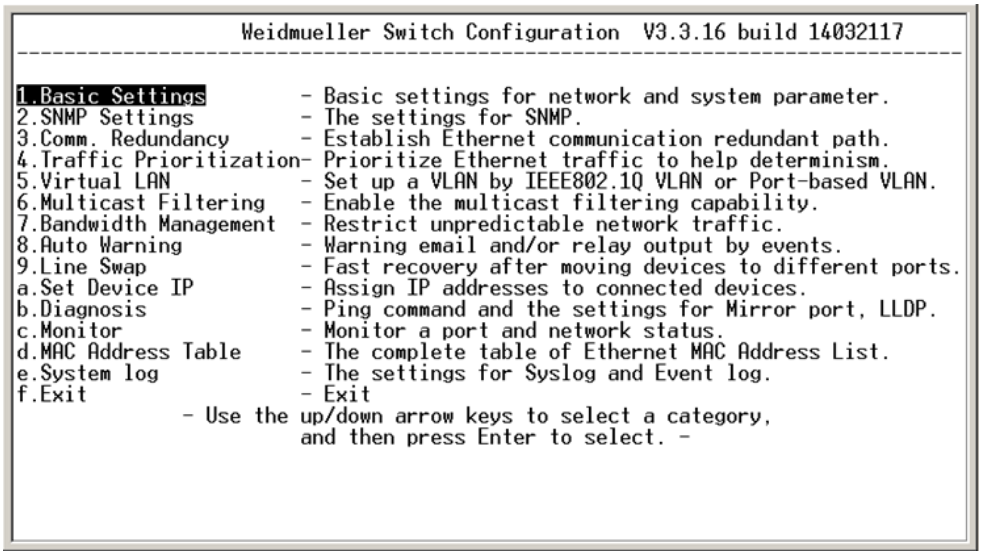
Type **1** to select **ansi/VT100** terminal type, and then press **Enter**.



The Console login screen will appear. Press **Enter** to open the Account pop-up selector and then select either **admin** (read/write access) or **user** (read access only). Use the keyboard's down arrow to move the cursor to the Password field, enter the default **Console Password "Detmold".** This password will be required to access any of the consoles (web, serial, Telnet). Leave the **Password** field blank if a console password has not been set), and then press **Enter**.



The **Main Menu** of the Switch´s serial console will be displayed.


Weidmueller Switch Configuration V3.3.16 build 14032117
1.Basic Settings - Basic settings for network and system parameter.
2.SNMP Settings - The settings for SNMP.
3.Comm. Redundancy - Establish Ethernet communication redundant path.
4.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
5.Virtual LAN - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
6.Multicast Filtering - Enable the multicast filtering capability.
7.Bandwidth Management - Restrict unpredictable network traffic.
8.Auto Warning - Warning email and/or relay output by events.
9.Line Swap - Fast recovery after moving devices to different ports.
a.Set Device IP - Assign IP addresses to connected devices.
b.Diagnosis - Ping command and the settings for Mirror port, LLDP.
c.Monitor - Monitor a port and network status.
d.MAC Address Table - The complete table of Ethernet MAC Address List.
e.System log - The settings for Syslog and Event log.
f.Exit - Exit
- Use the up/down arrow keys to select a category,
and then press Enter to select. -

After entering the **Main Menu**, use the following keys to move the cursor, and to select options.

Key	**Function**
Up/Down/Left/Right arrows, or Tab	Move the onscreen cursor
Enter	Display & select options
Space	Toggle options
Esc	Previous Menu

2.2 Configuration by Telnet Console

Opening the Weidmüller switch's Telnet or web console over a network requires that the PC host and Weidmüller switch are on the same logical subnet. You may need to adjust your PC host's IP address and subnet mask. By default, the Weidmüller switch's IP address is 192.168.1.110 and the switch's subnet mask is 255.255.255.0 (for a Class C network). If you do not change these values, and your PC host's subnet mask is 255.255.255.0, then its IP address must have the form 192.168.1.xxx

NOTE: When connecting to the switch's Telnet or web console ensure that your PC host and the switch are on the same logical subnet.

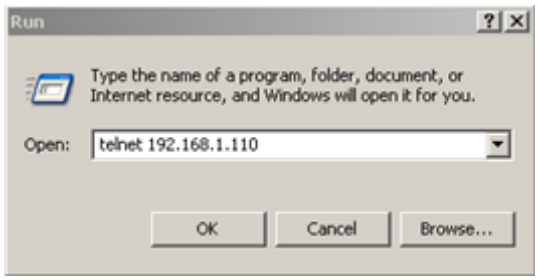
NOTE: When connecting to the switch's Telnet or web console, first connect one of the switch's Ethernet ports to your Ethernet LAN or directly to your PC's Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

NOTE: The Weidmüller switch's default IP address is **192.168.1.110**

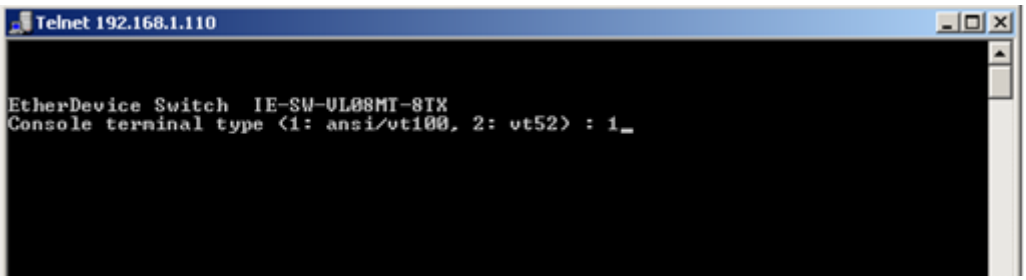
The default password is **Detmold**

After making sure that the Weidmüller switch is connected to the same LAN and logical subnet as your PC, open the Weidmüller switch's Telnet console as follows:

Click **Start → Run** from the Windows Start menu and then Telnet to the Weidmüller switch's IP address from the Windows **Run** window. You may also issue the Telnet command from a DOS prompt.



In the terminal window, the Telnet console will prompt you to select a terminal type. Type **1** to choose **ansi/vt100**, and then press **Enter**.



The Telnet console will prompt you to log in. Press **Enter** and then select **admin** (read/write access) or **user** (read access only)**.** Use the down arrow key on your keyboard to select the **Password** field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the **Password** field blank and press **Enter**.

The **Main Menu** of the Switch´s Telnet console will be displayed.

Telnet 192.168.1.110
Weidmueller Switch Configuration V3.3.16 build 14032117
1.Basic Settings - Basic settings for network and system parameter.
2.SNMP Settings - The settings for SNMP.
3.Comm. Redundancy - Establish Ethernet communication redundant path.
4.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
5.Virtual LAN - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
6.Multicast Filtering - Enable the multicast filtering capability.
7.Bandwidth Management - Restrict unpredictable network traffic.
8.Auto Warning - Warning email and/or relay output by events.
9.Line Swap - Fast recovery after moving devices to different ports.
a.Set Device IP - Assign IP addresses to connected devices.
b.Diagnosis - Ping command and the settings for Mirror port, LLDP.
c.Monitor - Monitor a port and network status.
d.MAC Address Table - The complete table of Ethernet MAC Address List.
e.System log - The settings for Syslog and Event log.
f.Exit - Exit
- Use the up/down arrow keys to select a category,
and then press Enter to select. -

After entering the **Main Menu**, use the following keys to move the cursor, and to select options.

Key	**Function**
Up/Down/Left/Right arrows, or Tab	Move the onscreen cursor
Enter	Display & select options
Space	Toggle options
Esc	Previous Menu

NOTE: The Telnet Console looks and operates in precisely the same manner as the RS-232 Console.

2.3 Accessing configuration interface via Web Browser

2.3.1 Accessing the Webinterface via HTTP

The Ethernet Switch's web browser interface provides a convenient way to modify the switch's configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft Internet Explorer 8.0 or higher with JVM (Java Virtual Machine) installed.

NOTE: To use the Switch's management and monitoring functions from a PC host connected to the same LAN as the switch, you must make sure that the PC host and the Switch are on the same logical subnet.

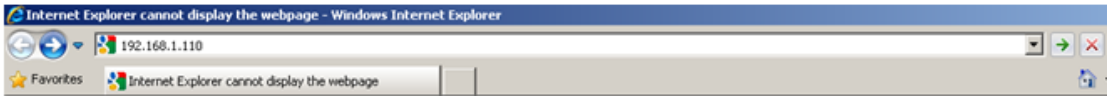
NOTE: If the Weidmüller switch is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

NOTE: Before accessing the Switch's web browser interface, first connect one of its RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can establish a connection with either a straight-through or cross-over Ethernet cable.

NOTE: The Weidmüller switch's default IP address is **192.168.1.110**.
The default password is **Detmold**

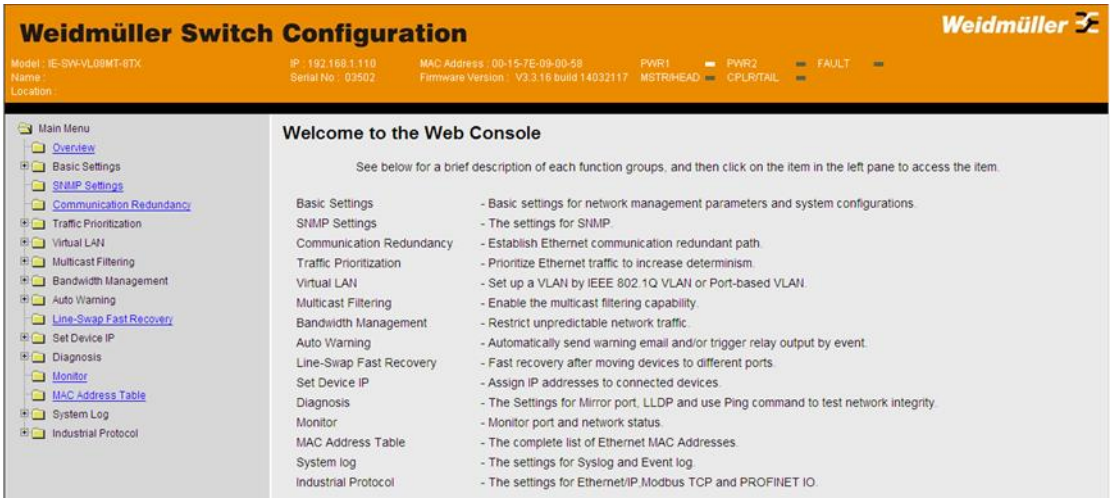
After making sure that the Weidmüller switch is connected to the same LAN and logical subnet as your PC, open the switch's web console as follows:

Open your web browser and type the Switch's IP address in the **Address** or **URL** field. Press **Enter** to establish the connection.


Internet Explorer cannot display the webpage - Windows Internet Explorer
192.168.1.110
Favorites
Internet Explorer cannot display the webpage

The web login page will open. Select the login account (admin or user) and enter the default **Password** "Detmold" (this is the same as the serial console or telnet password), and then click **Login** to continue. Leave the **Password** field blank if a password has not been set.

After logging in, you may need to wait a few moments for the web console to appear. Use the menu tree in the left navigation panel to open the function pages to access each of Ethernet Switch's functions.

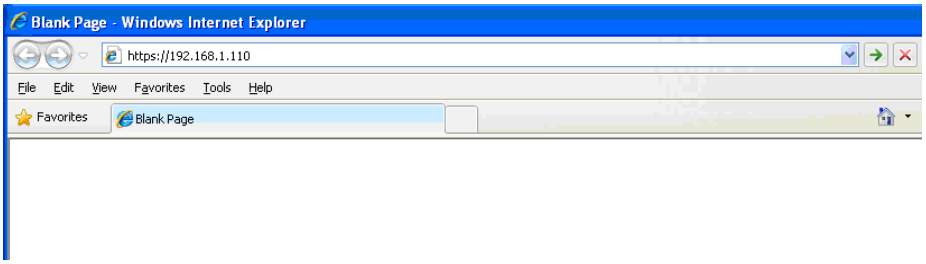

Weidmüller Switch Configuration
Weidmüller
Model : IE-SW-VL08MT-6TX
Name :
Location :
IP : 192.168.1.110
Serial No : 03502
MAC Address : 00-15-7E-09-00-58
Firmware Version : V3.3.16 build 14032117
PWR1
PWR2
FAULT
MSTR/HEAD
CPLR/TAIL
Main Menu
Overview
Basic Settings
SNMP Settings
Communication Redundancy
Traffic Prioritization
Virtual LAN
Multicast Filtering
Bandwidth Management
Auto Warning
Line-Swap Fast Recovery
Set Device IP
Diagnosis
Monitor
MAC Address Table
System Log
Industrial Protocol
Welcome to the Web Console
See below for a brief description of each function groups, and then click on the item in the left pane to access the item.
Basic Settings - Basic settings for network management parameters and system configurations.
SNMP Settings - The settings for SNMP.
Communication Redundancy - Establish Ethernet communication redundant path.
Traffic Prioritization - Prioritize Ethernet traffic to increase determinism.
Virtual LAN - Set up a VLAN by IEEE 802.1Q VLAN or Port-based VLAN.
Multicast Filtering - Enable the multicast filtering capability.
Bandwidth Management - Restrict unpredictable network traffic.
Auto Warning - Automatically send warning email and/or trigger relay output by event.
Line-Swap Fast Recovery - Fast recovery after moving devices to different ports.
Set Device IP - Assign IP addresses to connected devices.
Diagnosis - The Settings for Mirror port, LLDP and use Ping command to test network integrity.
Monitor - Monitor port and network status.
MAC Address Table - The complete list of Ethernet MAC Addresses.
System log - The settings for Syslog and Event log.
Industrial Protocol - The settings for Ethernet/IP,Modbus TCP and PROFINET IO.

2.3.2 Accessing the Webinterface via HTTPS

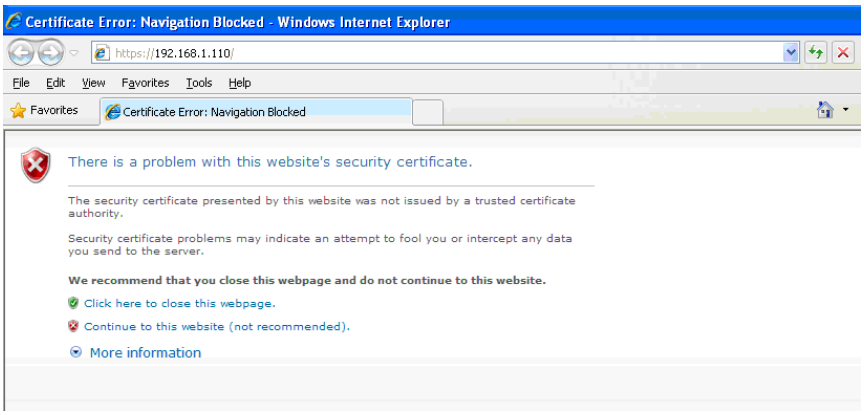
This function is not implemented in the Weidmüller Ethernet Switch Family “Value Line”.

To secure your HTTP access, the Weidmüller switch supports HTTPS/SSL to encrypt all HTTP traffic. Perform the following steps to access the Weidmüller switch web browser interface via HTTPS/SSL.

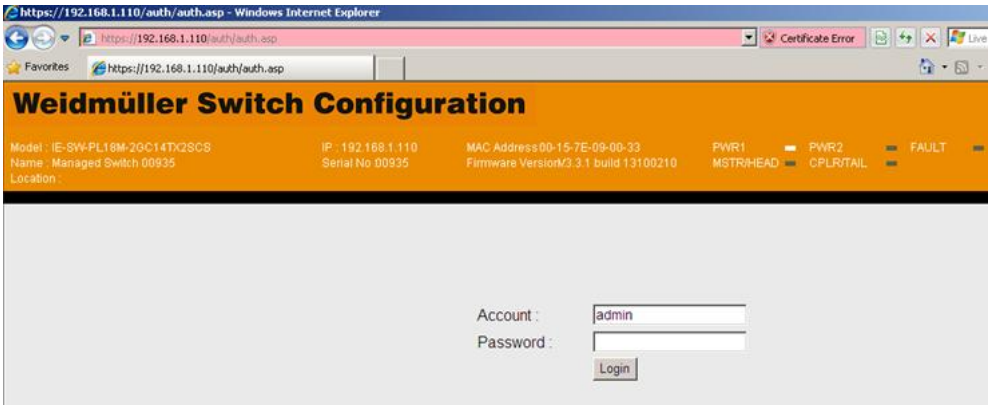
Open Internet Explorer and enter **https://<Switch´s IP address>** in the address field. Press Enter to establish the connection.



Warning messages will pop out to warn the user that the security certificate was issued by a company they have not chosen to trust.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.1.110/
File Edit View Favorites Tools Help
Favorites
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Select “**Continue to this website”** to enter the Weidmüller switch´s web browser interface and access the web browser interface secured via HTTPS/SSL.

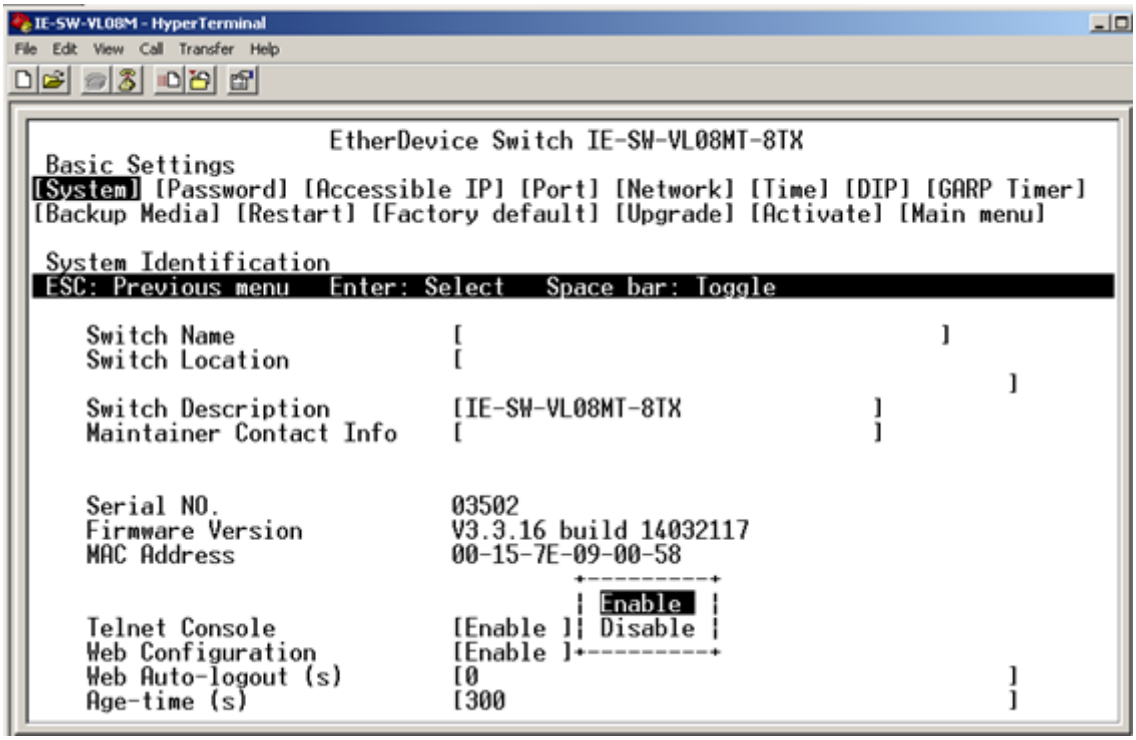


2.4 Accessing configuration interface via SSL

The console port can be accessed via a SSL/SSH connection using port 22. For configuration eg. a tool like PuTTY can be used. The procedure to configure the switch via SSL/SSH is the same as it has to be done for the serial interface.

2.5 Disabling Telnet and Browser Access

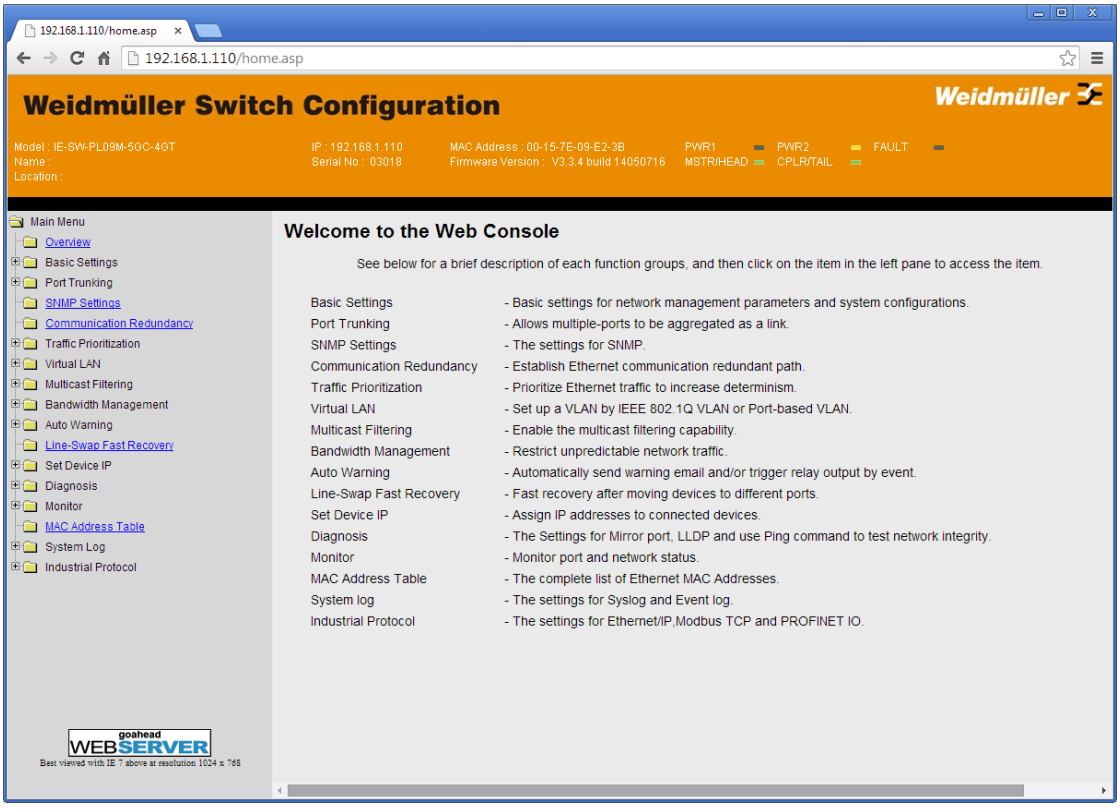
If you are connecting the Weidmüller Switch to a public network, but do not intend to use its management functions over the network, we suggest disabling both Telnet and Web consoles. This is done from the serial console by navigating to System Identification under Basic Settings. Disable or enable the Telnet Console and Web Configuration as shown below:



3. Featured Functions

In this chapter, we explain how to access the Weidmüller Switch's various configuration, monitoring, and administration functions. These functions can be accessed by serial, Telnet, or Web console. The serial console can be used if you do not know the Weidmüller Switch's IP address and requires that you connect the Weidmüller switch to a PC´s COM port. The Telnet and web consoles can be opened over an Ethernet LAN or the Internet.

The web console is the most user-friendly interface for configuring a Weidmüller Switch.


192.168.1.110/home.asp
Weidmüller Switch Configuration
Weidmüller
Model : IE-SW-PL09M-5GC-4GT
Name :
Location :
IP : 192.168.1.110
Serial No : 03018
MAC Address : 00-15-7E-09-E2-3B
Firmware Version : V3.3.4 build 14050716
PWR1
PWR2
FAULT
MSTR/HEAD
CPLR/TAIL
Main Menu
Overview
Basic Settings
Port Trunking
SNMP Settings
Communication Redundancy
Traffic Prioritization
Virtual LAN
Multicast Filtering
Bandwidth Management
Auto Warning
Line-Swap Fast Recovery
Set Device IP
Diagnosis
Monitor
MAC Address Table
System Log
Industrial Protocol
Welcome to the Web Console
See below for a brief description of each function groups, and then click on the item in the left pane to access the item.
Basic Settings - Basic settings for network management parameters and system configurations.
Port Trunking - Allows multiple-ports to be aggregated as a link.
SNMP Settings - The settings for SNMP.
Communication Redundancy - Establish Ethernet communication redundant path.
Traffic Prioritization - Prioritize Ethernet traffic to increase determinism.
Virtual LAN - Set up a VLAN by IEEE 802.1Q VLAN or Port-based VLAN.
Multicast Filtering - Enable the multicast filtering capability.
Bandwidth Management - Restrict unpredictable network traffic.
Auto Warning - Automatically send warning email and/or trigger relay output by event.
Line-Swap Fast Recovery - Fast recovery after moving devices to different ports.
Set Device IP - Assign IP addresses to connected devices.
Diagnosis - The Settings for Mirror port, LLDP and use Ping command to test network integrity.
Monitor - Monitor port and network status.
MAC Address Table - The complete list of Ethernet MAC Addresses.
System log - The settings for Syslog and Event log.
Industrial Protocol - The settings for Ethernet/IP,Modbus TCP and PROFINET IO.
goahead WEBSERVER
Best viewed with IE 7 above at resolution 1024 x 768

In this chapteIn this document we will use the Web interface for feature description. There are only a few differences between the web console, serial console, and Telnet console.

The following topics are covered in this chapter:

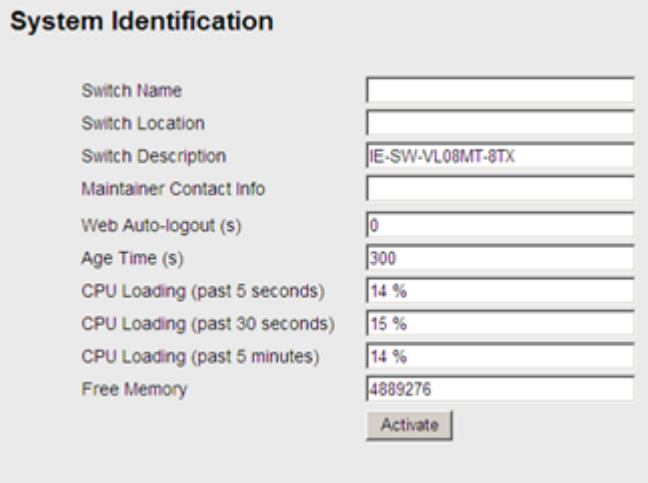
- Configuring Basic Settings
- Using Port Trunking (*Premium Line Models only*)
- Configuring SNMP
- Using PoE (*PoE Models only*)
- Using Communication Redundancy
- Using Traffic Prioritization
- Using Virtual LAN
- Using Multicast Filtering
- Using Bandwidth Management
- Using Auto Warning
- Using Line-Swap-Fast-Recovery
- Using Set Device IP
- Using Diagnosis
- Using Monitor
- Using the MAC Address Table
- Using System Log
- Using Industrial Protocols

3.1 Configuring Basic Settings

The Basic Settings section includes the most common settings required by administrators to maintain and control a Weidmüller switch.

3.1.1 System Identification

The system identification items are displayed at the top of the web page, and will be included in alarm emails. You can configure the System Identification items to make it easier to identify different switches that are connected to your network.



Switch Name

Setting	Description	Factory Default
Max. 30 characters	This option is useful for differentiating between the roles or applications of different units. Example: Factory Switch 1.	None

Switch Location

Setting	Description	Factory Default
Max. 80 characters	This option is useful for differentiating between the locations of different units. Example: Production line 1.	None

Switch Description

Setting	Description	Factory Default
Max. 30 characters	This option is useful for recording a more detailed description of the unit.	Name of type

Maintainer Contact Info

Setting	Description	Factory Default
Max. 30	This option is useful for providing information about who is responsible for maintaining this unit and how to	None

characters	contact this person.	

Web Auto-logout (sec)

Setting	Description	Factory Default
60 to 86400 (seconds)	Disable or extend the auto-logout time for the web management console.	0 (disabled)

Age Time (sec)

Setting	Description	Factory Default
15 to 3825 (seconds)	The length of time that a MAC address entry can remain in the Weidmüller switch´s MAC address table. When an entry reaches its aging time, it “ages out” and is purged from the switch, effectively cancelling frame forwarding to that specific port.	300

CPU Loading

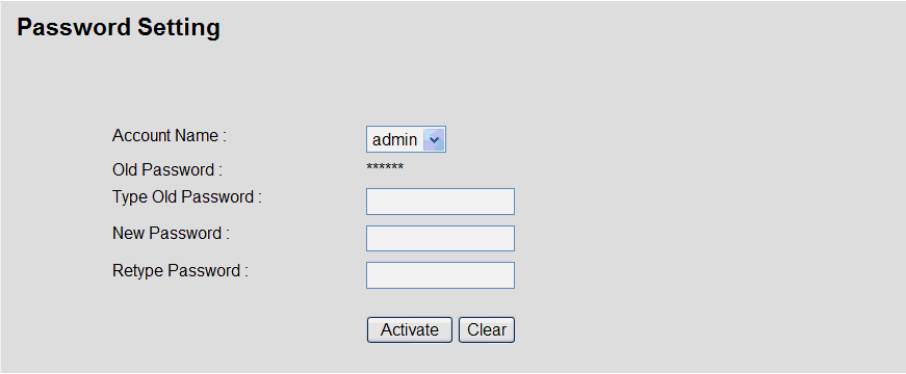
Setting	Description	Factory Default
Read-only	The CPU usage volume in the past 5 seconds, 30 seconds, and 5 minutes	None

Free Memory

Setting	Description	Factory Default
Read-only	The immediately free memory of the switch	None

3.1.2 Password

The Weidmüller switch provides two levels of access privileges. The **admin** account gives read/write access to all switch configuration parameters, and the **user** account gives read access only. A **user account** will only be able to view the configuration, but will not be able to make modifications.



NOTE: The Switch's default Password is ”Detmold”. If this Password is changed, then you will be required to type the new Password when logging into the serial console, Telnet console, or Web console.

Account

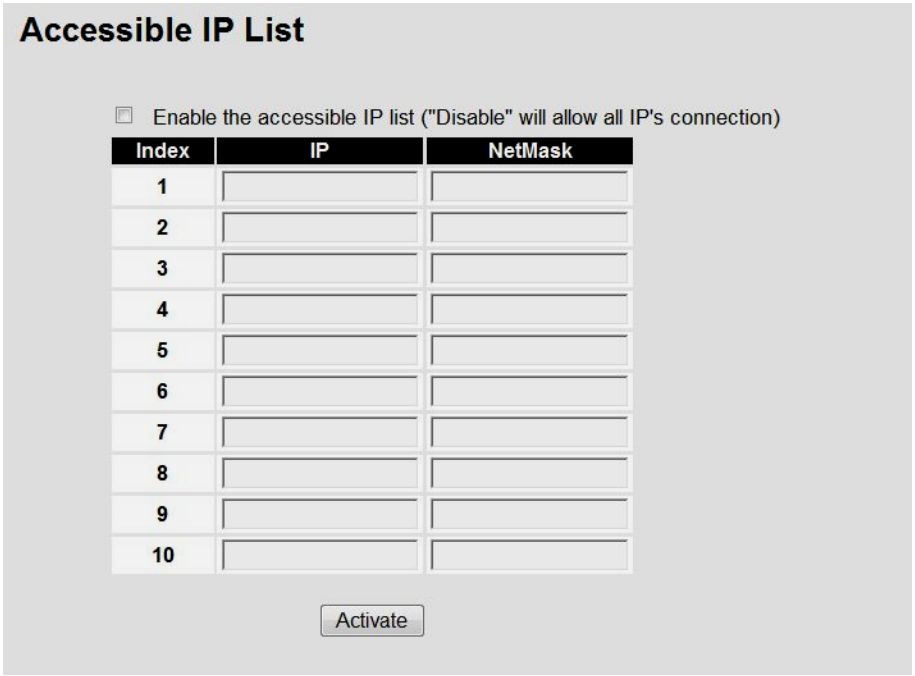
Setting	Description	Factory Default
admin	This account can modify the Weidmüller switch’s configuration.	**admin**
user	This account can only view the Weidmüller switch’s configurations.	

Password

Setting	Description	Factory Default
Old password (max. 16 characters)	Enter the current password	**Detmold**
New password (Max. 16 characters)	Enter the desired new password. Leave it blank if you want to remove the password.	None
Retype password (Max. 16 characters)	Enter the desired new password again. Leave it blank if you want to remove the password.	None

3.1.3 Accessible IP List

The Weidmüller switch uses an IP address-based filtering method to control access to the device.



You may add or remove IP addresses to limit access to the Weidmüller switch. When the accessible IP list is enabled, only addresses on the list will be allowed access to the Weidmüller switch. Each IP address and netmask entry can be tailored for different situations:

- **Grant access to one host with a specific IP address**
  For example, enter IP address 192.168.1.1 with netmask 255.255.255.255 to allow access to 192.168.1.1 only.
- **Grant access to any host on a specific subnetwork**
  For example, enter IP address 192.168.1.0 with netmask 255.255.255.0 to allow access to all IPs on the subnet defined by this IP address/subnet mask combination.
- **Grant access to all hosts**
  Make sure the accessible IP list is not enabled. Remove the checkmark from **Enable the accessible IP list**.

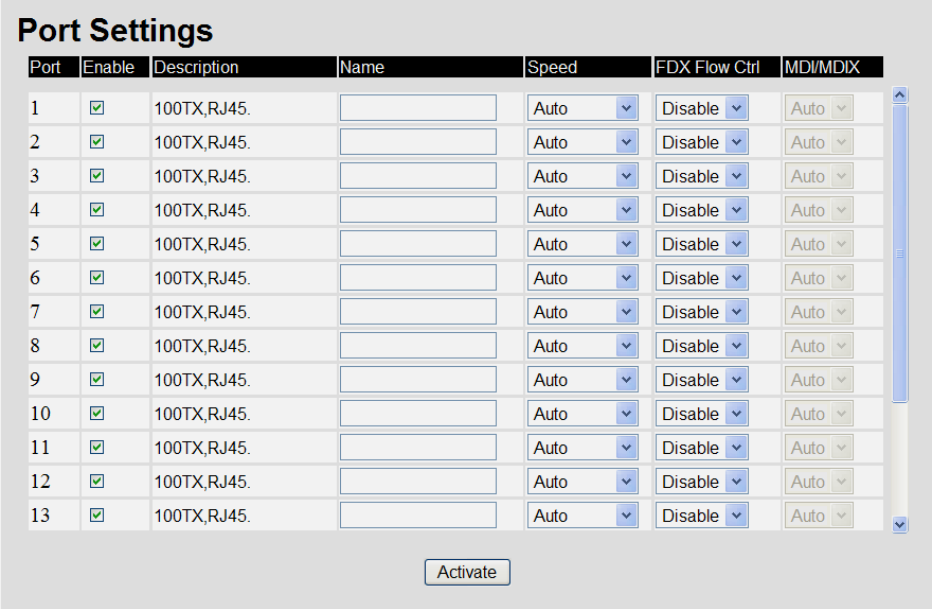
The following table shows additional configuration examples:

Hosts That Need Access	Input Format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

3.1.4 Port Settings

Ethernet Port Settings

Port settings are included to give the user control over Port Access, Port Transmission Speed, Flow Control, and Port Type (MDI or MDIX). An explanation of each configuration item follows:



Enable

Setting	Description	Factory Default
Checked	Allows data transmission through the port.	Enabled
Unchecked	Immediately shuts off port access.	

NOTE: If a connected device or sub-network is wreaking havoc on the rest of the network, the **Disable** option gives the administrator a quick way to shut off access through this port immediately.

Description

Setting	Description	Factory Default
Media type	Displays the media type for each module's port	N/A

Name

Setting	Description	Factory Default
Max. 63 characters	Specifies an alias for the port to help administrators differentiate between different ports. Example: PLC 1	None

Speed

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
1G-Full	Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	
100M-Full		
100M-Half		
10M-Full		
10M-Half		

FDX Flow Ctrl

This setting enables or disables flow control for the port when the port's Speed is set to Auto. The final result will be determined by the Auto process between the Weidmüller switch and connected devices.

Setting	Description	Factory Default
Enable	Enables flow control for this port when the port's Speed is set to Auto.	Disabled
Disable	Disables flow control for this port when the port's Speed is set to Auto.	

MDI/MDIX

Setting	Description	Factory Default
Auto	Allows the port to auto-detect the port type of the connected Ethernet device and change the port type accordingly.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-negotiating for port type.	
MDIX		

Note about Auto-Negotiation (possible lost of data packages in case of "Duplex mismatching")

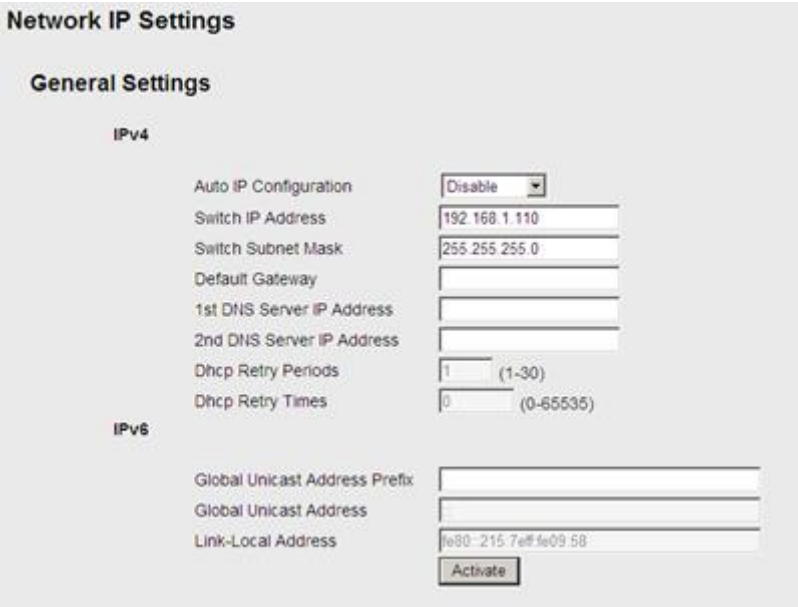
If an active AutoNeg-Port of the Switch is connected to a non-negotiating device, then the Switch will set its port transmission speed same as the connected device but is unable to correctly detect the duplex mode. As result the AutoNeg-port is set to the correct speed but is using always the half duplex mode as required by the IEEE 802.3u standard in such cases. For correct transmission between an AutoNeg-Port and a non-negotiating port the port with fixed values has to be set to half-duplex mode (speed either 10 or 100 Mbit/s).

3.1.5 Network Parameters

Network configuration allows users to configure both IPv4 and IPv6 parameters for management access over the network. The Weidmüller switch supports both IPv4 and IPv6, and can be managed through either of these address types.

.

See a brief explanation of each configuration item below.



IP4 Settings

The IPv4 settings include the switch's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server.

Auto IP Configuration

Setting	Description	Factory Default
Disable	The Weidmüller switch's IP address must be set manually.	Disable
By DHCP	The Weidmüller switch's IP address will be assigned automatically by the network's DHCP server.	
By BootP	The Weidmüller switch's IP address will be assigned automatically by the network's BootP server.	

Switch IP Address

Setting	Description	Factory Default
IP address for the Weidmüller Switch	Assigns the Weidmüller Switch´s IP address on a TCP/IP network.	192.168.1.110

Switch Subnet Mask

Setting	Description	Factory Default
Subnet mask for the Weidmüller Switch	Identifies the type of network to which the Switch is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

Default Gateway

Setting	Description	Factory Default
IP address for the gateway	The IP address of the router that connects the LAN to an outside network.	None

DNS IP Address

Setting	Description	Factory Default
1st DNS Server's IP address	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the Weidmüller Switch's URL (e.g., www.VL08M.company.com) in your browser's address field, instead of entering the IP address.	None
2nd DNS Server's IP address	The IP address of the secondary DNS Server used by your network. The Switch will use the 2nd DNS Server if the 1st DNS Server fails to connect.	None

DHCP Retry Periods

Setting	Description	Factory Default
1 to 30	Users can configure the DHCP retry period manually	1

DHCP Retry Times

Setting	Description	Factory Default
0 to 65535	Users can configure the times of DHCP retry manually	0

IP6 Settings

IPv6 setting includes two distinct address types—Link-Local Unicast address and Global Unicast address. A Link-Local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. To connect to a larger network with multiple segments, the switch must be configured with a Global Unicast address.

Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway

Setting	Description	Factory Default
Global Unicast Address Prefix	The prefix value must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.	None

Global Unicast Address

Setting	Description	Factory Default
None	Displays the IPv6 Global Unicast address. The network portion of the Global Unicast address can be configured by specifying the Global Unicast Prefix and using an EUI-64 interface ID in the low order 64 bits. The host portion of the Global Unicast address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address).	None

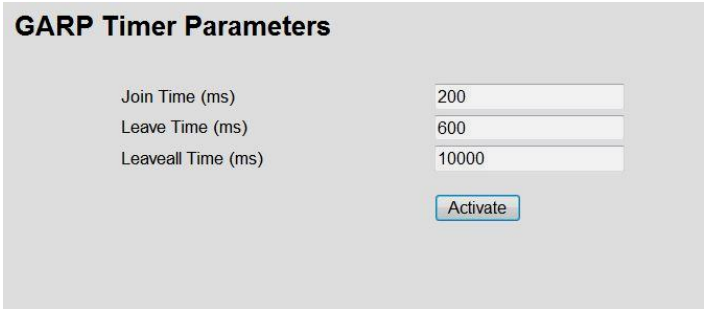
Link-Local Address

Setting	Description	Factory Default
None	The network portion of the Link-Local address is FE80 and the host portion of the Link-Local address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address)	FE80 :: (EUI-64 form of the MAC address)

Neighbor Cache

Setting	Description	Factory Default
None	The information in the neighbor cache that includes the neighboring node's IPv6 address, the corresponding Link-Layer address, and the current state of the entry.	None

3.1.6 GARP Timer Parameters



Join Time

Setting	Description	Factory Default
None	Specifies the period of the join time	200

Leave Time

Setting	Description	Factory Default
None	Specifies the period of leave time	600

Leaveall Time

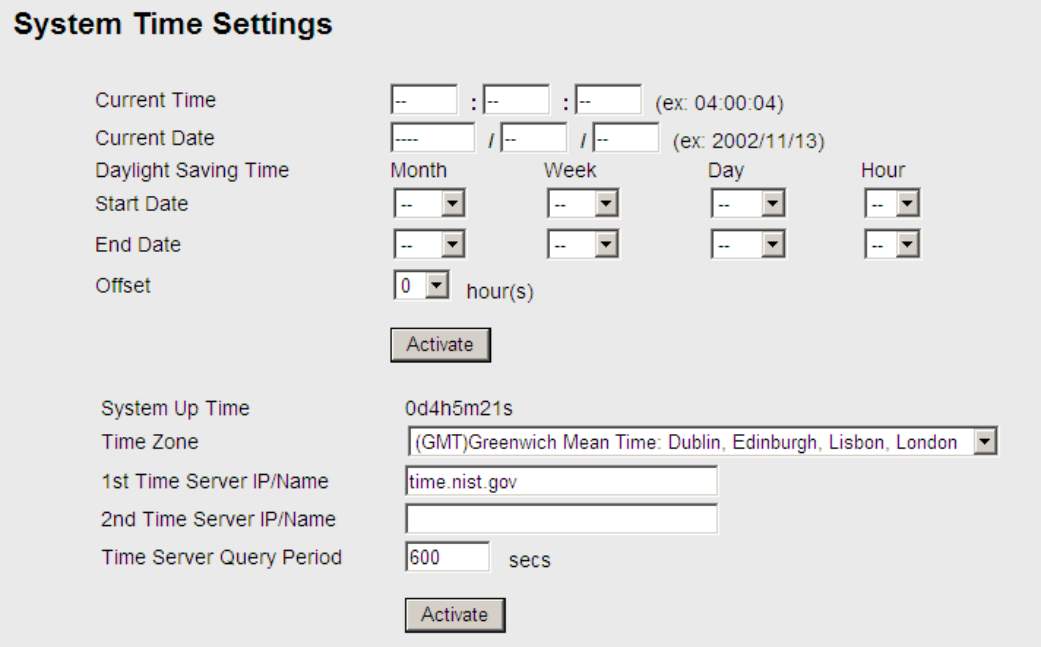
Setting	Description	Factory Default
None	Specifies the period of leaveall time	10000

NOTE **Leave Time** should be at least two times more than **Join Time**, and **Leaveall Time** should be larger than **Leave Time**.

3.1.7 Time

3.1.7.1 System Time Settings

The **Time** configuration page lets users set the time, date, and other settings. An explanation of each setting is given below the figure.



The Weidmüller switch has a time calibration function based on information from an NTP server or user specified time and date. Functions such as automatic warning emails can therefore include time and date stamp.

NOTE: The Weidmüller switch does not have a real time clock. The user must update the Current Time and Current Date to set the initial time for the Weidmüller switch after each reboot, especially when the network does not have an Internet connection for an NTP server or there is no NTP server on the LAN.

Current Time

Setting	Description	Factory Default
User-specified time.	Allows configuration of the local time in local 24-hour format.	None

Current Date

Setting	Description	Factory Default
User-specified date.	Allows configuration of the local date in yyyy-mm-dd format.	None

Daylight Saving Time

The Daylight Saving Time settings are used to automatically set the Weidmüller switch's time forward according to national standards.

Start Date

Setting	Description	Factory Default
User-specified date.	Specifies the date that Daylight Saving Time begins.	None

End Date

Setting	Description	Factory Default
User-specified date.	Specifies the date that Daylight Saving Time ends.	None

Offset

Setting	Description	Factory Default
User-specified hour.	Specifies the number of hours that the time should be set forward during Daylight Saving Time.	None

System Up Time

Indicates how long the Weidmüller switch remained up since the last cold start.

Time Zone

Setting	Description	Factory Default
User selectable time zone	Specifies the time zone, which is used to determine the local time offset from GMT (Greenwich Mean Time).	GMT (Greenwich Mean Time)

NOTE: Changing the time zone will automatically correct the current time. Be sure to set the time zone before setting the time.

Time Server IP/Name

Setting	Description	Factory Default
1st Time Server IP/Name	IP or Domain address (e.g., 192.168.1.1 or time.stdtime.gov.tw or time.nist.gov).	time.nist.gov
2nd Time Server IP/Name	The Weidmüller Switch will try to locate the 2nd NTP Server if the 1st NTP Server fails to connect.	

3.1.7.2 IEEE 1588 PTP

NOTE:

Protocol 1588 PTP is not implemented in the Weidmüller "Value Line" managed Switches.

The following information is taken from the NIST website at http://ieee1588.nist.gov/intro.htm:

"Time measurement can be accomplished using the IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems (IEEE 1588-2008) to synchronize real-time clocks incorporated within each component of the electrical power system for power automation applications.

IEEE 1588, which was published in November 2002, expands the performance capabilities of Ethernet networks to control systems that operate over a communication network. In recent years an increasing number of electrical power systems have been using a more distributed architecture with network technologies that have less stringent timing specifications. IEEE 1588 generates a master-slave relationship between the clocks, and enforces the specific timing requirements in such

power systems. All devices ultimately get their time from a clock known as the grandmaster clock. In its basic form, the protocol is intended to be administration free."

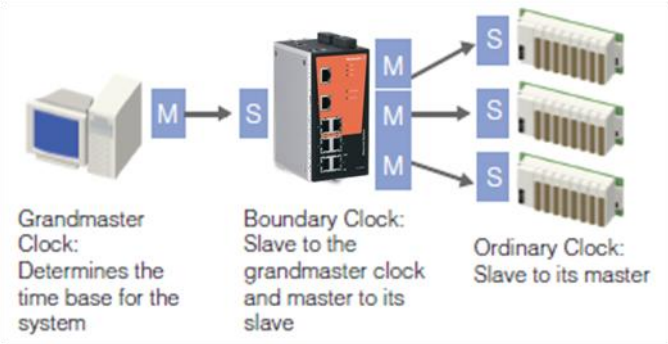
How does an Ethernet switch affect 1588 synchronization?

The following content is taken from the NIST website at http: //ieee1588.nist.gov/switch.htm:

"An Ethernet switch potentially introduces multi-microsecond fluctuations in the latency between the 1588 grandmaster clock and a 1588 slave clock. Uncorrected these fluctuations will cause synchronization errors. The magnitude of these fluctuations depends on the design of the Ethernet switch and the details of the communication traffic. Experiments with prototype implementations of IEEE 1588 indicate that with suitable care the effect of these fluctuations can be successfully managed. For example, use of appropriate statistics in the 1588 devices to recognized significant fluctuations and use suitable averaging techniques in the algorithms controlling the correction of the local 1588 clock will be the good design means to achieve the highest time accuracy."

Can Ethernet switches be designed to avoid the effects of these fluctuations?

A switch can be designed to support IEEE 1588 while avoiding the effects of queuing. In this case two modifications to the usual design of an Ethernet switch are necessary:



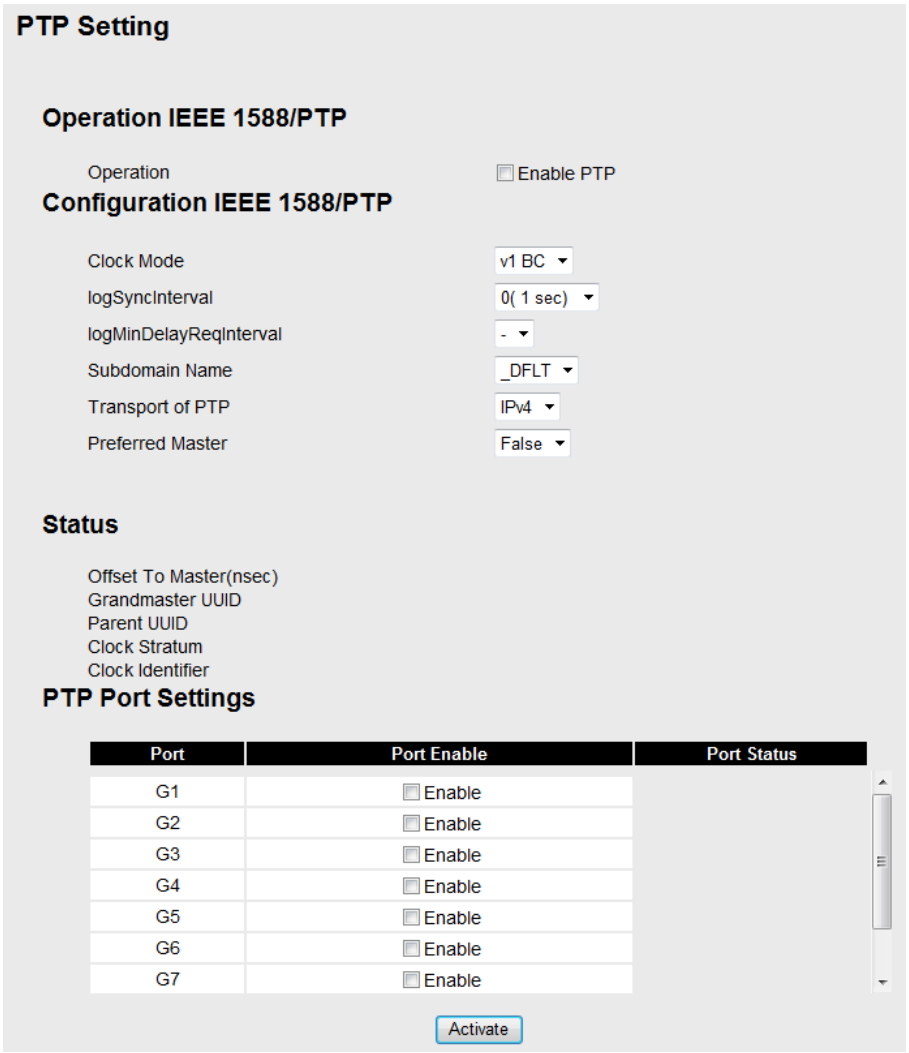
The **Boundary Clock and Transparent Clock** functionalities defined by IEEE 1588 must be implemented in the switch.

The switch must be configured such that it does not pass IEEE 1588 message traffic using the normal communication mechanisms of the switch.

Such an Ethernet switch will synchronize clocks directly connected to one of its ports to the highest possible accuracy.

NOTE: The Weidmüller Premium Line managed Switches only supports software-based IEEE 1588 PTP V1.

Configuring PTP



IEEE 1588/PTP Operation

Operation

Setting	Description	Factory Default
Enable PTP	Globally disables or enables IEEE 1588 operation.	Disabled

Clock Mode (sets the switch's clock mode)

Setting	Description	Factory Default
v1 BC	Operates as an IEEE 1588 v1 boundary clock.	v1 BC

logSyncInterval (sets the synchronization message time interval)

Setting	Description	Factory Default
0, 1, 2, 3, or 4	0 (1 s), 1 (2 s), 2 (4 s), 3 (8 s), or 4 (16 s). Supported in IEEE 1588 V1.	0

logMinDelayReqInterval

Setting	Description	Factory Default
0, 1, 2, 3, 4, or 5	Minimum delay request message interval	0 (1 sec.)

Subdomain Name

Setting	Description	Factory Default
_DFLT (0), _ALT(1), _ALT(2), or _ALT(3)	Subdomain name (IEEE 1588-2002) or the domain Number (IEEE 1588-2008) fields in PTP messages	_DFLT (0)

Transport of PTP (transport protocol of an IEEE 1588 PTP message)

Setting	Description	Factory Default
IPv4	IEEE 1588 PTP V1 supports IPv4 only	IPv4

Preferred Master

Setting	Description	Factory Default
True or False	Set this switch to be the Grand Master.	False

Status

Setting	Description	Factory Default
N/A	Shows the current IEEE 1588 PTP status.	N/A

PTP Port Settings

Shows the current switch PTP port settings.

3.1.8 Turbo Ring DIP Switch (Menu item and DIP switches)

The menu item **Turbo Ring DIP Switch** can be used as follows:

- Enable or disable the settings for Turbo Ring redundancy by the 4 DIP switches located on the top of the Switch housing.
- Selection of used redundancy protocol **Turbo Ring V1** or **Turbo Ring V2** if enabled in this menu.

Turbo Ring DIP Switch
Disable the Turbo Ring DIP Switch
1. To enable the entire set of Hardware DIP switches, uncheck the "Disable the Turbo Ring DIP Switch" option.
2. To disable the entire set of Hardware DIP switches, check the "Disable the Turbo Ring DIP Switch" option.
Set DIP switch as Turbo Ring
Set DIP switch as Turbo Ring V2
Activate

By default **Turbo Ring V2** is activated and will be used when configuring Turbo Ring redundancy by DIP switches (as shown in above screenshot).

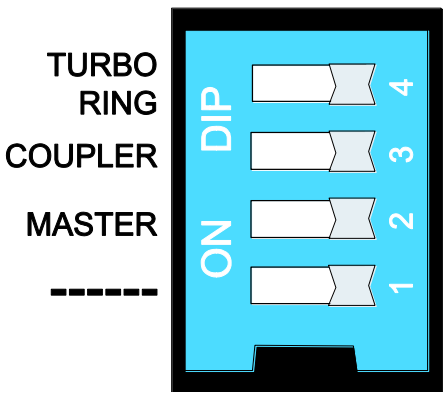
Turbo Ring DIP Switches are supported by all Weidmüller managed Switches

except Premium Line switch series 16/18-Ports (IE-SW-PL16M / IE-SW-PL18M)

For a detailed description of **Turbo Ring V1** and **Turbo Ring V2** please refer to chapter **Using Communication Redundancy.**

Configuring a Turbo Ring by external DIP Switches

- The external DIP switches only can be used if they are **not** disabled in menu *'Turbo Ring DIP Switch'* (default value).
- By factory defaults the Turbo Ring DIP Switches are set to the OFF position.
- Turbo Ring (either V1 or V2) will be activated immediately (without reboot) when setting DIP switch 4 to ON.
- The used Turbo Ring version depends on parameter 'Set DIP switch as Turbo Ring…' in Webinterface menu *'Turbo Ring DIP Switch*'



- If DIP switch 4 is set to ON then the Webinterface menu *'Communication Redundancy'* is locked, showing the selected Turbo Ring version. DIP switch 4 overrules the redundancy settings of the Webinterface.
- The role of the switch (Master yes/no, Coupler yes/no) will be set by DIP switches 2 and 3.

Behavior of DIP Switch settings when protocol is set to 'Turbo Ring V1'

DIP 1	DIP 2	DIP 3	DIP 4
Reserved for future use.	ON: Enables this SWITCH as the Ring Master.	ON: Enables the default "Ring Coupling" ports.	ON: Activates DIP switches 1, 2, 3 to configure **Turbo Ring** settings.
	OFF: This SWITCH will not be the Ring Master.	OFF: Do not use this SWITCH as the ring coupler.	OFF: DIP switches 1, 2, 3 will be disabled.

Behavior of DIP Switch settings when protocol is set to 'Turbo Ring V2'

DIP 1	DIP 2	DIP 3	DIP 4
ON: Enables the default "Ring Coupling (backup)" port.	ON: Enables this SWITCH as the Ring Master.	ON: Enables the default "Ring Coupling" port.	ON: Activates DIP switches 1, 2, 3 to configure **Turbo Ring V2** settings.
OFF: Enables the default "Ring Coupling (primary)" port.	OFF: This SWITCH will not be the Ring Master.	OFF: Do not use this SWITCH as a ring coupler.	OFF: DIP switches 1, 2, 3 will be disabled.

Regarding the used ports for Ring redundancy and Ring coupling please refer to section Communication redundancy (Chapter 3.5.3.1 Configuring Turbo Ring V1, Chapter 3.5.3.2 Configuring Turbo Ring V2).

By factory defaults the Turbo Ring DIP Switches are set to the **OFF position**.

The Turbo Ring Ports and Coupling Ports will be added automatically to all VLANs if you set DIP Switch 4 to the "ON" position.

If you do not enable any of the managed Weidmüller Ethernet Switches to be the Ring Master, the Turbo Ring protocol will automatically choose the Ethernet Switch with the smallest MAC address range to be the Ring Master. If you accidentally enable more than one Ethernet Switch to be the Ring Master, these switches will auto-negotiate to determine which one will be the Ring Master.

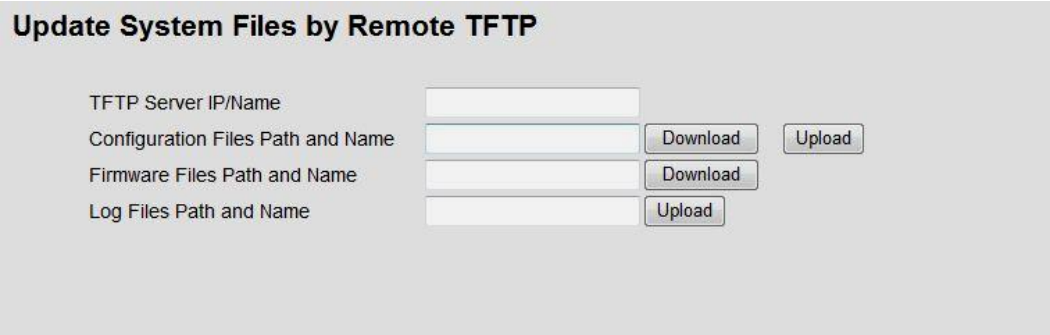
If you use the browser interface to enable the DIP switches (by un-checking the “Disable the Turbo Ring DIP switch” checkbox), and then flip DIP switch 4 from **ON** to **OFF**, the Ring Ports and Coupling Ports that were added to all VLANs will be restored to their previous software settings. (For details, please refer to the “Using Virtual LANs” section of this manual).

3.1.9 System File Update (Firmware and Configuration)

3.1.9.1 Update System Files by Remote TFTP

Following saving and restoring functions are available via a remote TFTP server:

- Upload the current configuration to remote TFTP server
- Download the current configuration from remote TFTP server
- Download new firmware from remote TFTP server (The information how to download new firmware is described in **Appendix C)**.
- Upload the current logging data to remote TFTP server



TFTP Server IP/Name

Setting	Description	Factory Default
IP Address of TFTP Server	Specifies the IP address or name of the remote TFTP server. Must be set up before downloading or uploading files.	None

Configuration Files Path and Name

Setting	Description	Factory

		Default
Max. 40 characters	Specifies the path and file name of the Weidmüller switch's configuration file on the TFTP server.	None

Firmware Files Path and Name

Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the Weidmüller switch's firmware file.	None

Log Files Path and Name

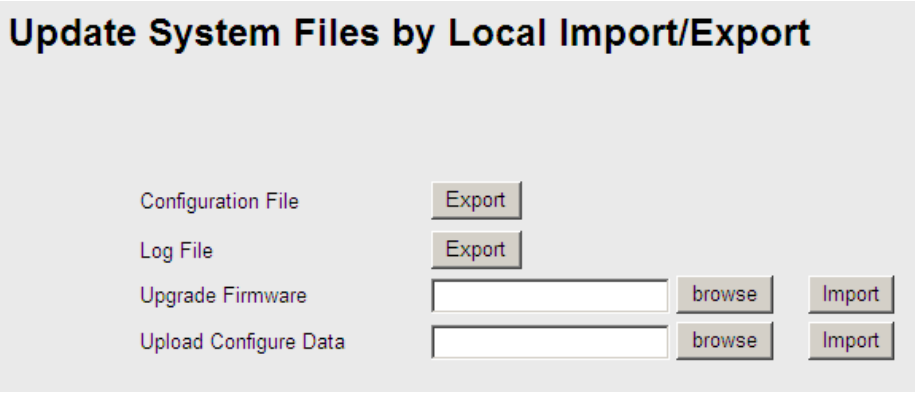
Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the Weidmüller switch's log file.	None

After setting the desired path and file names, click **Download** to download the prepared file from the remote TFTP server, or click **Upload** to upload the desired file to the remote TFTP server.

3.1.9.2 Update System Files by Local Import/Export

Following saving and restoring functions are available via file-based data transfer:

- Export the current configuration to connected PC
- Export the current logging data
- Upgrade of firmware by importing a firmware file (*.rom). The information how to download new firmware is described in **Appendix C.**
- Loading a new configuration by importing a configuration file



Configuration File

To export the configuration file of the Ethernet Switch, click **Export** to save it to the local host.

Log File

To export the Log file of the Ethernet Switch, click **Export** to save it to the local host.

NOTE: Some operating systems will open the configuration file and log file directly in the web page. In such cases, right click the Export button to save the file.

Upgrade Firmware

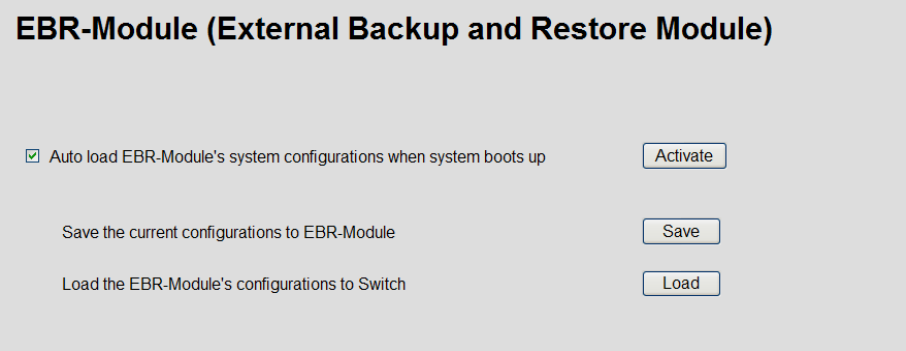
To import a new firmware file into the Weidmüller switch, click **Browse** to select the firmware file that is saved on your computer. The upgrade procedure will proceed automatically after clicking **Import**.

Upload Configure Data

To import a configuration file into the Weidmüller switch, click **Browse** to select the configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking button *Import*.

3.1.9.3 System File Update by EBR-Module

You can use Weidmüller´s External Backup and Restore Module (can be ordered separately under article no.: 1241430000) to save and load the Weidmüller switch's configurations using the switch's RS-232 console port (RJ45 connector on top of the housing).


EBR-Module (External Backup and Restore Module)
Auto load EBR-Module's system configurations when system boots up
Activate
Save the current configurations to EBR-Module
Save
Load the EBR-Module's configurations to Switch
Load

Auto load EBR-Module´s system configurations when system boots up

Setting	Description	Factory Default
Enable	Enables Auto load system configurations from EBR-Module when system boots up	Enable
Disable	Disables Auto load system configurations from EBR-Module when system boots up	

If enabled the configuration of a connected EBR-Module will be loaded and saved automatically into the Switch when the device is booting.

Save the current configurations to the EBR-Module

To export the current configuration file of the Weidmüller switch, click on button **Save** to save it to the EBR-Module.

Load the EBR-Module's configurations to the Switch

To import the configuration file into the Weidmüller switch, click button **Load** to load it to the Switch.

If you want to use an EBR-Module to import the configuration of Switch A (stored in the EBR-Module) into Switch B then both models must be of the same type.

3.1.10 Security

The Security software function's
- **RADIUS and TACACS+ for user login authentication**
- **RADIUS for 802.1x port authentication**

are only available for Weidmüller *Premium Line* managed switches.

Security can be categorized in two levels: the user name/password level, and the port access level. For user name/password level security, Weidmüller switches provide two different user login options: Terminal Access Controller Access-Control System Plus (TACACS+) and Remote Authentication Dial In User Service (RADIUS). The TACACS+ and RADIUS mechanism is a centralized "AAA" (Authentication, Authorization and Accounting) system for connecting to network services. The fundamental purpose of both TACACS+ and RADIUS is to provide an efficient and secure mechanism for user account management.

3.1.10.1 User Login Authentication

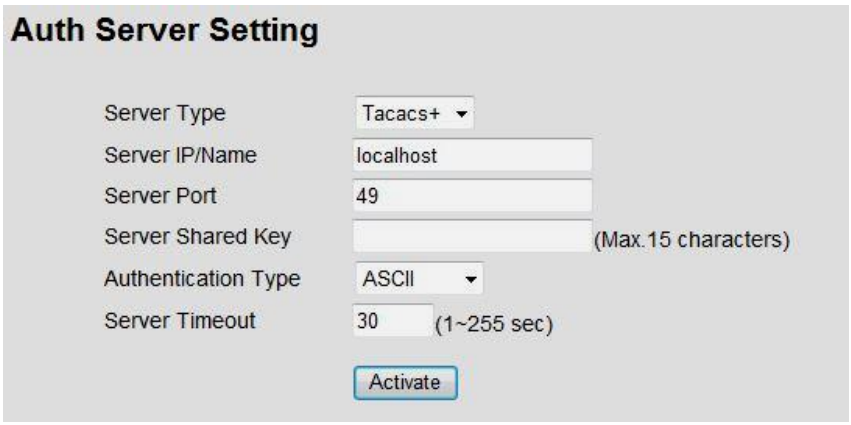
User Login Settings

Both TACAS+ and RADIUS authentication are available options.

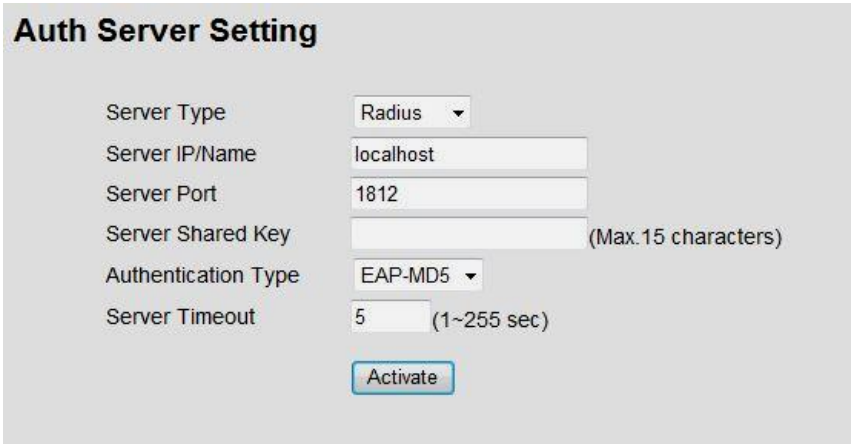
Auth Server Setting

The detailed configuration settings of TACACS+ and RADIUS are displayed in the table below:

Server type TACACS+



Server type Radius



Setting	Description	Factory Default
Server Type	Authentication server types selection	TACACS+
Server IP/Name	Set IP address of an external TACACS+/RADIUS server as the authentication database	Localhost
Server Port	Set communication port of an external TACACS+/RADIUS server as the authentication database	TACACS+ : 49 RADIUS : 1812
Server Shared Key	Set specific characters for server authentication verification	None
Authentication Type	The authentication mechanism is EAP-MD5 for RADIUS	ASCII for TACACS+
Server Timeout	The timeout period to wait for a server response	TACACS+ : 30 RADIUS : 5

3.1.10.2 Using Port Access Control

The Weidmüller **Premium** Line switches provide two kinds of Port-Based Access Control:

- **Static Port Lock**
- **IEEE 802.1X**

Static Port Lock

In this case the Weidmüller switch can be configured to protect static MAC addresses for a specific port. With the Port Lock function, these locked ports will not learn any additional addresses, but only allow traffic from preset static MAC addresses, helping to block hackers and careless usage.

Access control according IEEE 802.1X

The IEEE 802.1X standard defines a protocol for client/server-based access control and authentication. The protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet, and which otherwise would be readily accessible. The purpose of the authentication server is to check each client that requests access to the port. The client is only allowed access to the port if the client's permission is authenticated.

Three components are used to create an authentication mechanism based on 802.1X standards: Client/Supplicant, Authentication Server, and Authenticator.

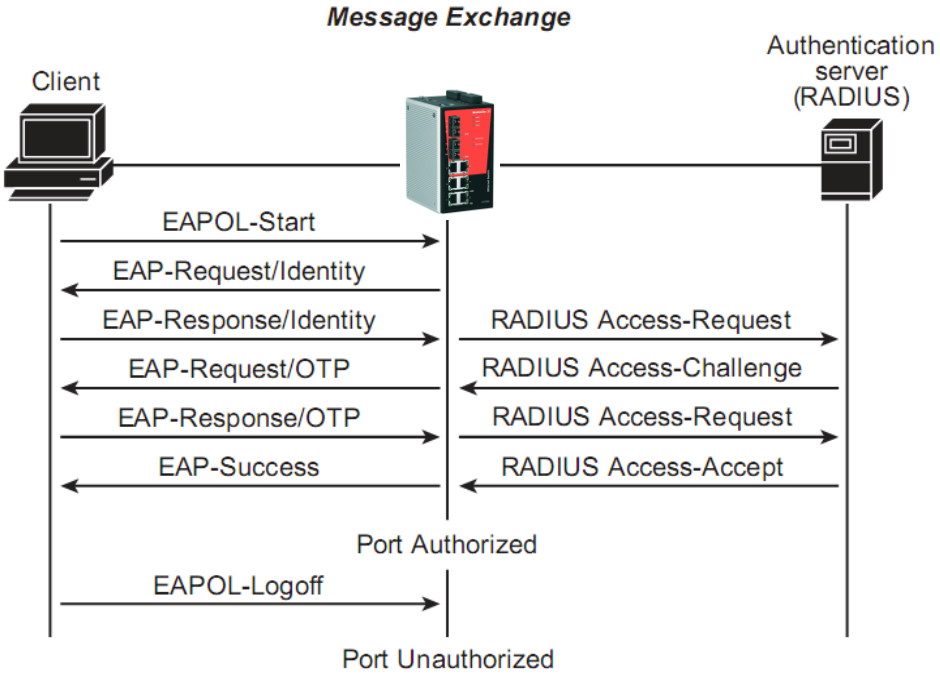
Client/Supplicant: The end station that requests access to the LAN and switch services and responds to the requests from the switch.

Authentication server: The server that performs the actual authentication of the supplicant.

Authenticator: Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant.

The Weidmüller switch acts as an authenticator in the 802.1X environment. A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server, or implement the authentication server in the Weidmüller switch by using a Local User Database as the authentication look-up table. When we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames between each other.

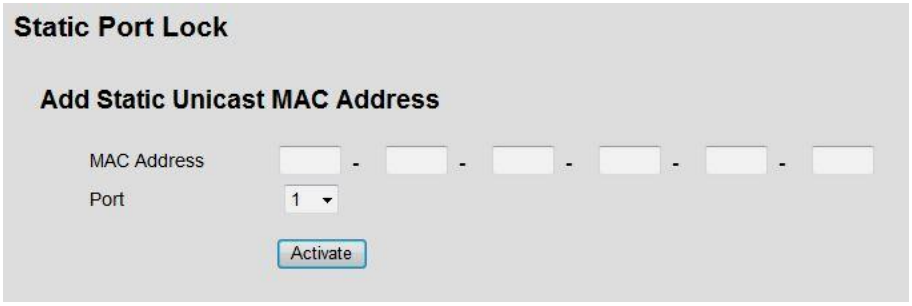
Authentication can be initiated either by the supplicant or the authenticator. When the supplicant initiates the authentication process, it sends an **EAPOL-Start** frame to the authenticator. When the authenticator initiates the authentication process or when it receives an **EAPOL Start** frame, it sends an **EAP Request/Identity** frame to ask for the username of the supplicant. The following actions are described below:



1. When the supplicant receives an "EAP Request/Identity" frame, it sends an "EAP Response/Identity" frame with its username back to the authenticator.
2. If the RADIUS server is used as the authentication server, the authenticator relays the "EAP Response/Identity" frame from the supplicant by encapsulating it into a "RADIUS Access-Request" frame and sends to the RADIUS server. When the authentication server receives the frame, it looks up its database to check if the username exists. If the username is not present, the authentication server replies with a "RADIUS Access-Reject" frame to the authenticator if the server is a RADIUS server or just indicates failure to the authenticator if the Local User Database is used. The authenticator sends an "EAP-Failure" frame to the supplicant.
3. The RADIUS server sends a "RADIUS Access-Challenge," which contains an "EAP Request" with an authentication type to the authenticator to ask for the password from the client. RFC 2284 defines several EAP authentication types, such as "MD5-Challenge," "One-Time Password," and "Generic Token Card." Currently, only "MD5-Challenge" is supported. If the Local User Database is used, this step is skipped.
4. The authenticator sends an "EAP Request/MD5-Challenge" frame to the supplicant. If the RADIUS server is used, the "EAP Request/MD5-Challenge" frame is retrieved directly from the "RADIUS Access-Challenge" frame.
5. The supplicant responds to the "EAP Request/MD5-Challenge" by sending an "EAP Response/MD5-Challenge" frame that encapsulates the user's password using the MD5 hash algorithm.
6. If the RADIUS server is used as the authentication server, the authenticator relays the "EAP Response/MD5-Challenge" frame from the supplicant by encapsulating it into a "RADIUS Access-Request" frame along with a "Shared Secret," which must be the same within the authenticator and the RADIUS server, and sends the frame to the RADIUS server. The RADIUS server checks against the password with its database, and replies with "RADIUS Access-Accept" or "RADIUS Access-Reject" to the authenticator. If the Local User Database is used, the password is checked against its database and indicates success or failure to the authenticator.
7. The authenticator sends "EAP Success" or "EAP Failure" based on the reply from the authentication server.

Configuring Static Port Lock

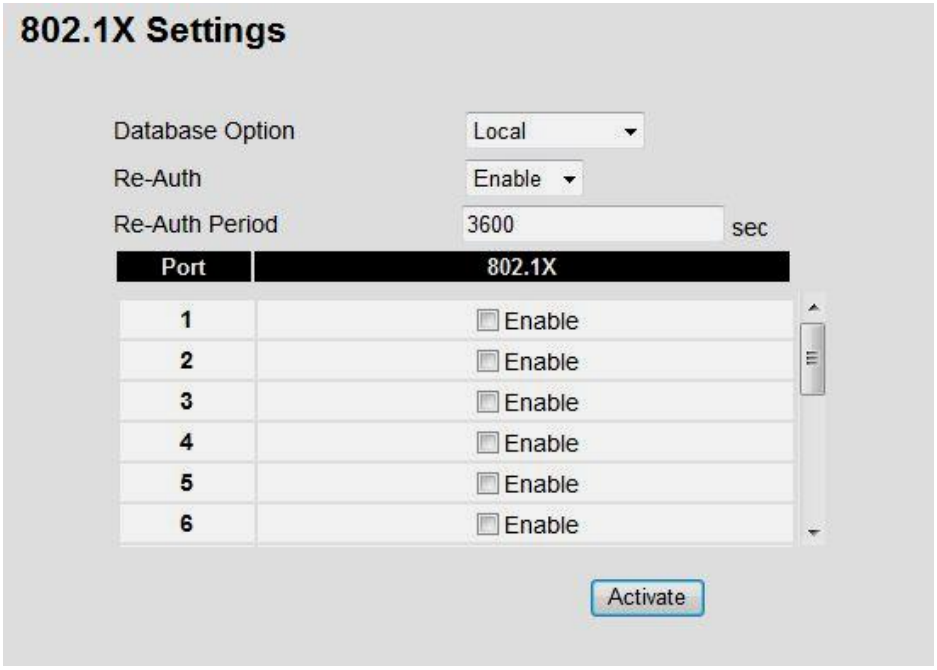
The Weidmüller switch supports adding unicast groups manually if required.



Static Unicast MAC Address

Setting	Description	Factory Default
MAC Address	Add the static unicast MAC address into the address table.	None
Port	Associates the static address with a dedicated port.	1

Configuring IEEE 802.1X



Database Option

Setting	Description	Factory Default
Local	Select this option when setting the Local User	Local

(Max. 32 users)	Database as the authentication database.	
Radius	Select this option to set an external RADIUS server as the authentication database. The authentication mechanism is EAP-MD5.	Local
Radius, Local	Select this option to make using an external RADIUS server as the authentication database the first priority. The authentication mechanism is EAP-MD5 The first priority is to set the Local User Database as the authentication database.	Local

Radius Server

Setting	Description	Factory Default
IP address or domain name	The IP address or domain name of the RADIUS server	local host

Server Port

Setting	Description	Factory Default
Numerical	The UDP port of the RADIUS server	1812

Shared Key

Setting	Description	Factory Default
alphanumeric (Max. 40 characters)	A key to be shared between the external RADIUS server and the Weidmüller switch. Both ends must be configured to use the same key.	None

Re-Auth

Setting	Description	Factory Default
Enable/Disable	Select enable to require re-authentication of the client after a preset time period of no activity has elapsed.	Disable

Re-Auth Period

Setting	Description	Factory Default
Numerical (60 to 65535 sec)	Specify how frequently the end stations need to reenter usernames and passwords in order to stay connected.	3600

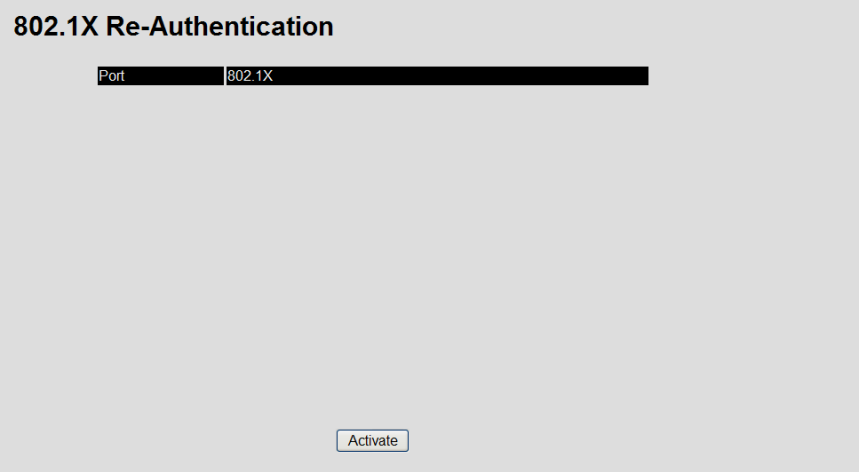
802.1X

Setting	Description	Factory Default
Enable/Disable	Checkmark the checkbox under the 802.1X column to	Disable

	enable IEEE 802.1X for one or more ports. All end stations must enter usernames and passwords before access to these ports is allowed.	

802.1X Re-Authentication

The Weidmüller switch can force connected devices to be re-authorized manually.

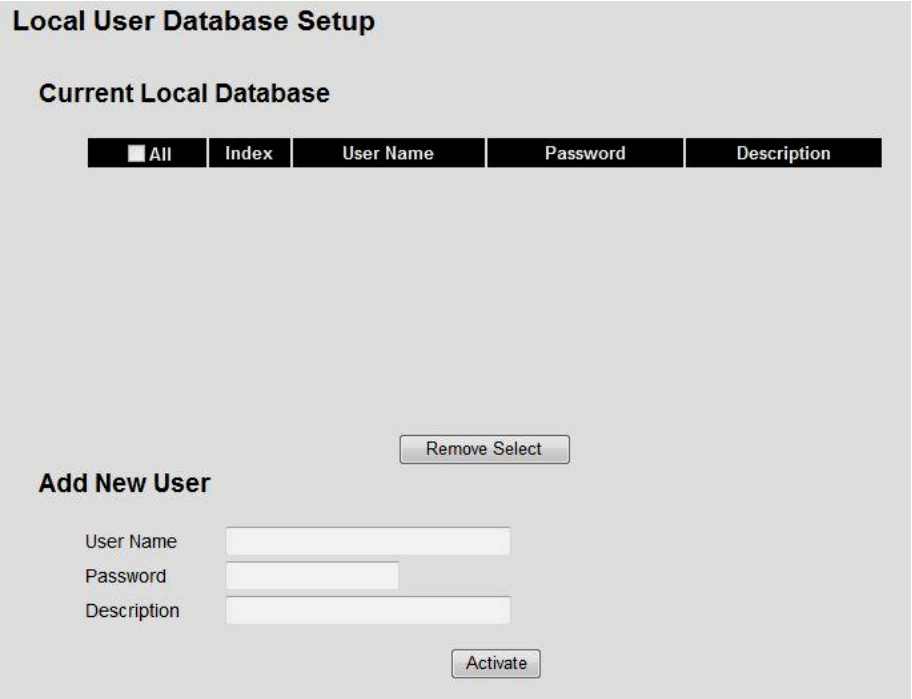


802.1X Re-Authentication

Setting	Description	Factory Default
Enable/Disable	Enables or disables 802.1X Re-Authentication	Disable

Local User Database Setup

When setting the Local User Database as the authentication database, set the database first.

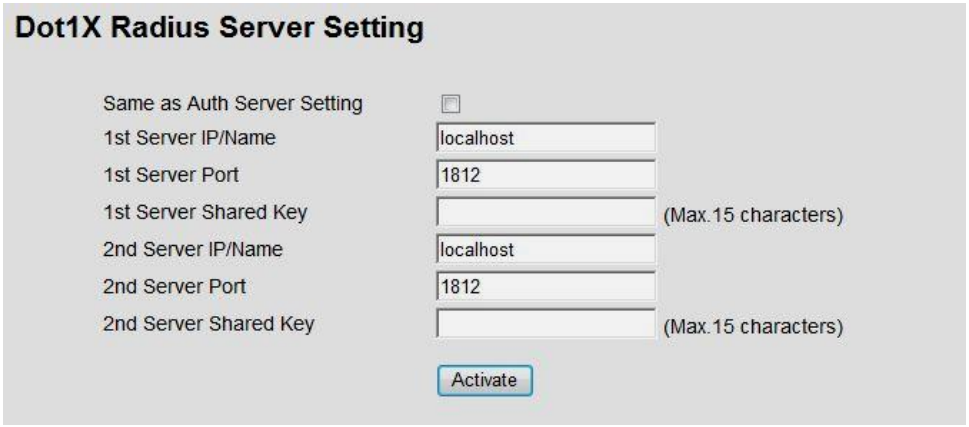


Local User Database Setup

Setting	Description	Factory Default
User Name (Max. 30 characters)	User Name for the Local User Database	None
Password (Max. 16 characters)	Password for the Local User Database	None
Description (Max. 30 characters)	Description for the Local User Database	None

NOTE: The user name for the Local User Database is **case-insensitive**.

Dot1X Radius Server Setting



Same as Auth Server Setting

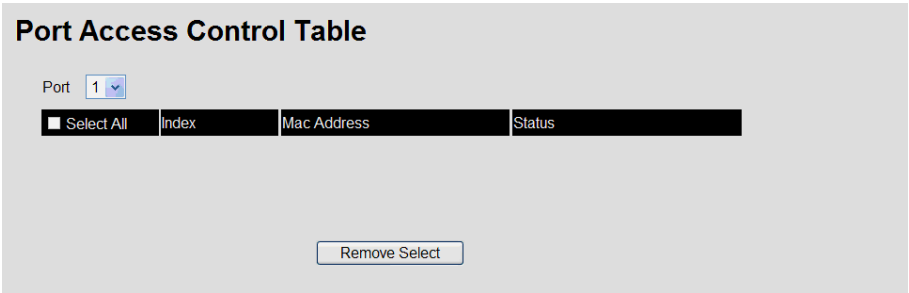
Setting	Description	Factory Default
Enable/Disable	Enable to use the same setting as Auth Server	Disable

Server Setting

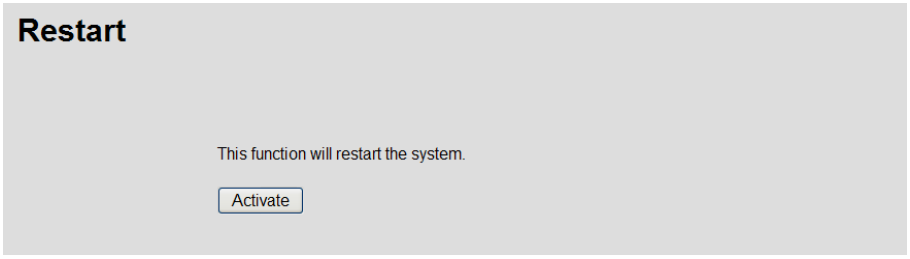
Setting	Description	Factory Default
Server IP/Name	Specifies the IP/name of the server	localhost
Server Port	Specifies the port of the server	1812
Server Shared Key	Specifies the shared key of the server	None

Port Access Control Table

The port status will indicate whether the access is authorized or unauthorized.

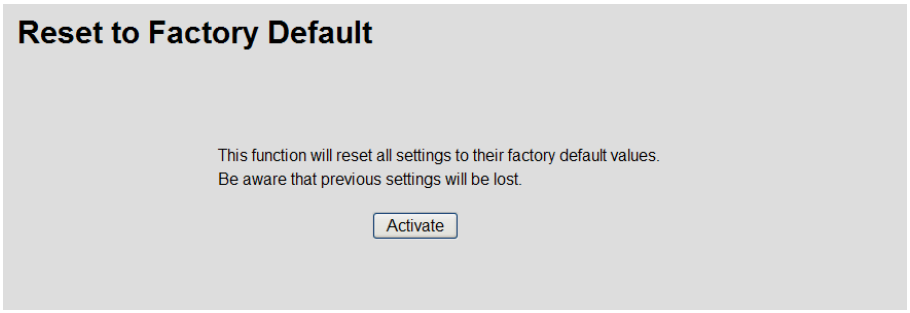


3.1.11 Restart



This function is used to restart the Ethernet Switch.

3.1.12 Factory Default


Reset to Factory Default
This function will reset all settings to their factory default values.
Be aware that previous settings will be lost.
Activate

This function provides users with a quick way of restoring the Weidmüller switch's configuration to factory defaults. The function is available in the serial, Telnet, and web consoles.

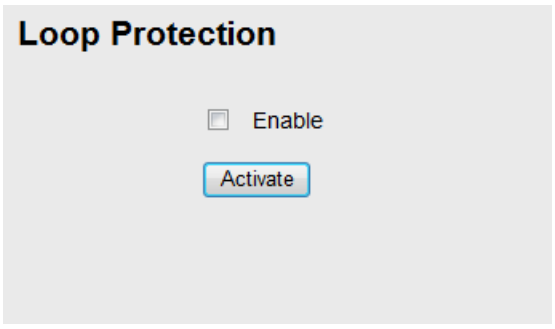
NOTE: After restoring the factory default configuration, you will need to use the default network settings to re-establish the web or Telnet console connection with the Weidmüller switch.

3.1.13 Loop Protection

Avoid maintenance/installation crews from mistakenly placing one cable on the same switch generating a loop problem.

Two ports that are looped will be blocked if the loop happens on the switch itself.

If triggered then the fault LED will light up.



3.2 Using Port Trunking

Port Trunking is only available for Weidmüller *Premium Line* managed switches.

Link Aggregation allows one or more links to be aggregated together to form a Link Aggregation Group. A MAC client can treat Link Aggregation Groups as if they were a single link.

The Weidmüller switch's Port Trunking feature allows devices to communicate by aggregating up to 4 trunk groups, with a maximum of 8 ports for each group. If one of the 8 ports fails, the other seven ports will provide back up and share the traffic automatically.

Port Trunking can be used to combine up to 8 ports between two Weidmüller switches. If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 1600 Mbps.

The Port Trunking Concept

The Port Trunking protocol provides the following benefits:

- Gives you more flexibility in setting up your network connections, since the bandwidth of a link can be doubled, tripled, or quadrupled.
- Provides redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.
- Load sharing—MAC Client traffic may be distributed across multiple links.

To avoid broadcast storms or loops in your network while configuring a trunk, first disable or disconnect all ports that you want to add to the trunk or remove from the trunk. After you finish configuring the trunk, enable or re-connect the ports.

If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be up to 1.6 Gbps on the Weidmüller switch. This means that users can connect one Weidmüller switch to another Weidmüller switch by Port Trunking to double, triple, or quadruple the bandwidth of the connection.

Important note about Port Trunking:

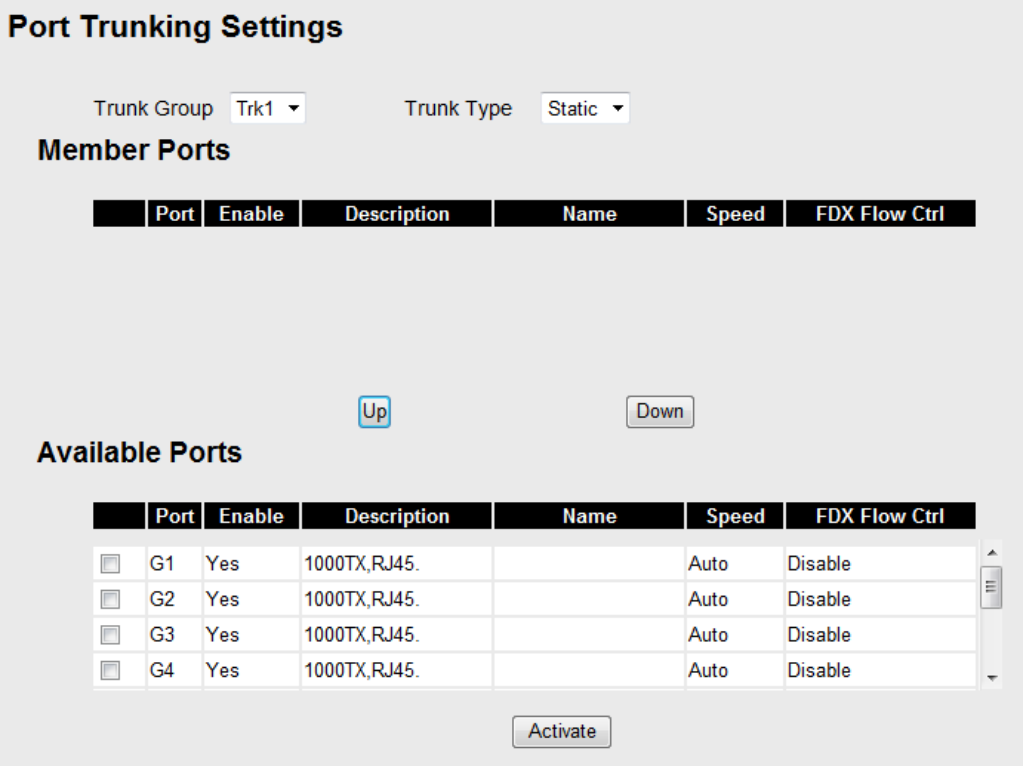
Each Premium Line Weidmüller switch can set a maximum of 4 Port Trunking groups (Trk1/Trk2/Trk3/Trk4). When you activate Port Trunking, certain settings related to the trunking ports will be reset to factory default values, or disabled:

- Communication Redundancy will be reset
- Traffic Prioritization will be reset
- Port-based VLAN or 802.1Q VLAN will be reset
- Multicast Filtering will be reset
- Port Lock will be reset and disabled
- Set Device IP will be reset
- Mirror Port will be reset

After port trunking has been activated, you can configure these settings again for each trunking port.

3.2.1 Port Trunking Settings

The **Port Trunking Settings** page is used to assign ports to a Trunk Group.



Step 1: Select the desired **Trunk Group (Trk1, Trk2, Trk3, Trk4) from the** drop-down box .

Step 2: Select Static, or LACP from the **Trunk Type** drop-down box.

Step 3: Select the desired ports under **Available Ports** and click **Up** to add to the Trunk group.

Step 4: Select the desired ports under **Member Ports** and click **Down** to remove from the group.

Trunk Group (maximum of 4 trunk groups)

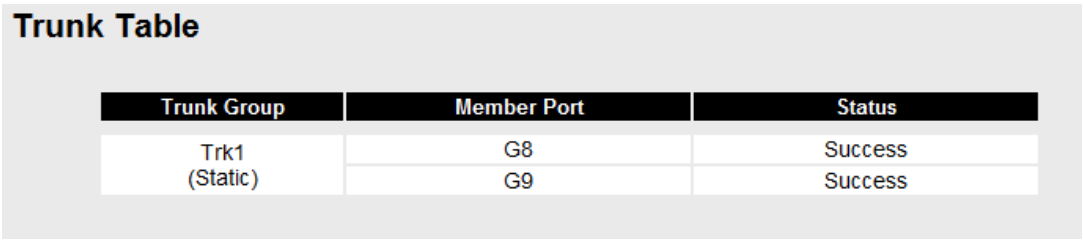
Setting	Description	Factory Default
Trk1, Trk2, Trk3, Trk4	Specifies the current trunk group	Trk1

Trunk Type

Setting	Description	Factory Default
Static	Selects proprietary trunking protocol	Static
LACP	Selects LACP (IEEE 802.3ad, Link Aggregation Control Protocol).	Static

Available Ports/Member Ports

Setting	Description	Factory Default
Member/Available ports	Lists the ports in the current trunk group and the ports that are available to be added.	N/A
Check box	Selects the port to be added or removed from the group.	Unchecked
Port	Port number.	N/A
Port description	Displays the media type for each port.	N/A
Name	Displays the specified name for each port.	N/A
Speed	Indicates the transmission speed for each port (1G-Full, 100M-Full, 100M-Half, 10M-Full, or 10M-Half)	N/A
FDX flow control	Indicates if the FDX flow control of this port is "Enabled" or "Disabled."	N/A
Up	Add selected ports into trunk group from available ports.	N/A
Down	Remove selected ports from Member Ports (trunk group) to available ports.	N/A



Trunk Table

Setting	Description
Trunk group	Displays the Trunk Type and Trunk Group.
Member port	Display which member ports belong to the trunk group.
Status	Success means port trunking is working properly. Fail means port trunking is not working properly.

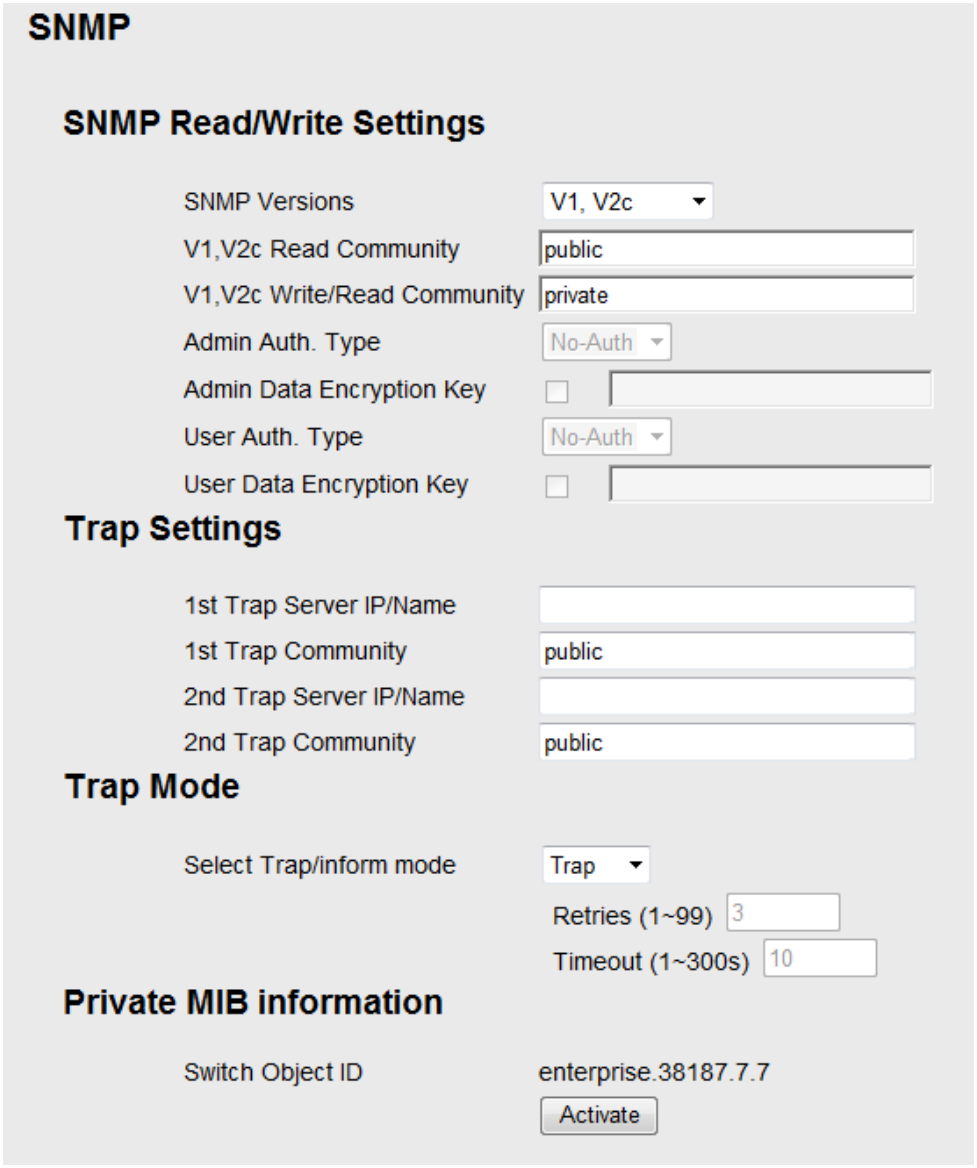
3.3 Configuring SNMP

Weidmüller managed Switches supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community strings *public* and *private* by default. SNMP V3 requires that you select an authentication level of MD5 or SHA, and is the most secure protocol. You can also enable data encryption to enhance data security.

Supported SNMP security modes and levels are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication.
SNMP V3	No-Auth	No	No	Uses an account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

These parameters are configured on the SNMP page. A more detailed explanation of each parameter is given below the figure.



3.3.1 SNMP Read/Write Settings

SNMP Versions

Setting	Description	Factory Default
V1, V2c, V3, or V1, V2c, or V3 only	Specifies the SNMP protocol version used to manage the switch.	V1, V2c

V1, V2c Read Community

Setting	Description	Factory Default

Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read-only access. The SNMP agent will access all objects with read-only permissions using this community string.	Public

V1, V2c Write/Read Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read/write access. The SNMP server will access all objects with read/write permissions using this community string.	Private

For SNMP V3, there are two levels of privileges for different accounts to access the Weidmüller switch. **Admin** privilege allows access and authorization to read and write the MIB file. **User** privilege allows reading the MIB file only.

Admin Auth. Type (for SNMP V1, V2c, V3 and V3 only)

Setting	Description	Factory Default
No-Auth	Allows the admin account to access objects without authentication.	No
MD5-Auth	Authentication will be based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

Admin Data Encryption Key (for SNMP V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key (between 8 and 30 characters).	No
Disable	Specifies that data will not be encrypted.	No

User Auth. Type (for SNMP V1, V2c, V3 and V3 only)

Setting	Description	Factory Default
No-Auth	Allows the admin account and user account to access objects without authentication.	No
MD5-Auth	Authentication will be based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No

SHA-Auth	Authentication will be based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

User Data Encryption Key (for SNMP V1, V2c, V3 and V3 only)

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key (between 8 and 30 characters).	No
Disable	No data encryption	No

3.3.2 Trap Settings

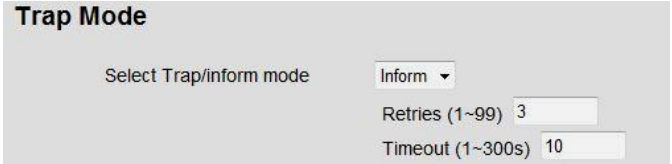
SNMP traps allow an SNMP agent to notify a Network Management System (NMS) of a significant event. The switch supports two SNMP modes, **Trap** mode and **Inform** mode.

SNMP Trap Mode “Trap”

In Trap mode, the SNMP agent sends an SNMPv1 trap PDU to the NMS. No acknowledgment is sent back from the NMS so the agent has no way of knowing if the trap reached the NMS.

SNMP Trap Mode “Inform”

SNMPv2 provides an inform mechanism. When an inform message is sent from the SNMP agent to the NMS, the receiver sends a response to the sender acknowledging receipt of the event. This behavior is similar to that of the get and set requests. If the SNMP agent does not receive a response from the NMS for a period of time, the agent will resend the trap to the NMS agent. The maximum timeout time is 300 sec (default is 10 sec), and the maximum number of retries is 99 times (default is 3 time). When the SNMP agent receives acknowledgement from the NMS, it will stop resending the inform messages.



1st Trap Server IP/Name

Setting	Description	Factory Default
IP or name	Specifies the IP address or name of the primary trap server used by your network.	None

1st Trap Community

Setting	Description	Factory Default
character string	Specifies the community string to use for authentication (maximum of 30 characters).	public

2nd Trap Server IP/Name

Setting	Description	Factory Default
IP or name	Specifies the IP address or name of the secondary trap server used by your network.	None

2nd Trap Community

Setting	Description	Factory Default
character string	Specifies the community string to use for authentication (maximum of 30 characters).	public

Inform Mode Select

Setting	Description	Factory Default
Retries	Enter Inform Retry number	3
Timeout	Enter Inform Timeout window	10

3.3.3 Private MIB Information

Switch Object ID

Setting	Description	Factory Default
Specific Weidmüller Switch ID	Indicates the Weidmüller switch's enterprise value.	Depends on the switch model type

NOTE: The Switch Object ID cannot be changed.

3.4 Using PoE (PoE Models Only)

Power over Ethernet has become increasingly popular due in large part to the reliability provided by PoE Ethernet switches that supply the necessary power to Powered Devices (PD) when AC power is not readily available or cost-prohibitive to provide locally.

Power over Ethernet can be used with:

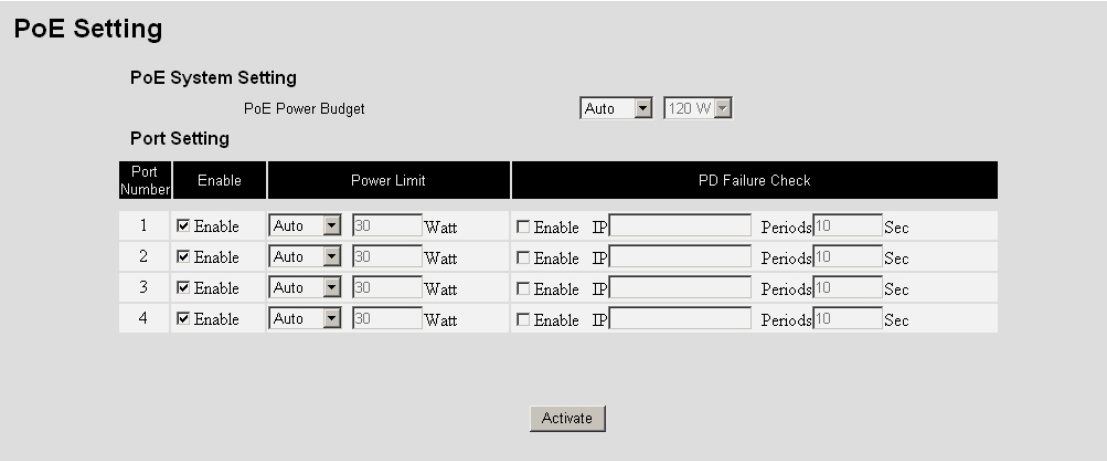
- Surveillance cameras
- Security I/O sensors
- Industrial wireless access points
- Emergency IP phones

In fact, it's not uncommon for video, voice, and high-rate industrial application data transfers to be integrated into one network. Weidmüller's PoE switches are equipped with many advanced PoE management functions, providing vital security systems with a convenient and reliable Ethernet network. Moreover, Weidmüller's PoE switches support the high power PoE+ standard (IEEE 802.3at), 24 VDC direct power input, and 20 ms fast recovery redundancy, Turbo Ring and Turbo Chain.

3.4.1 PoE Settings

The settings are included to give the user control over the system's PoE power budget, PoE port access, PoE port power limit and PD failure check.

An explanation of each configuration item follows:


PoE Setting
PoE System Setting
PoE Power Budget
Auto
120 W
Port Setting
Port Number
Enable
Power Limit
PD Failure Check
1 Enable Auto 30 Watt Enable IP Periods 10 Sec
2 Enable Auto 30 Watt Enable IP Periods 10 Sec
3 Enable Auto 30 Watt Enable IP Periods 10 Sec
4 Enable Auto 30 Watt Enable IP Periods 10 Sec
Activate

PoE Power Budget

Indicates the PoE power that can be supplied by the system

Setting	Description	Factory Default
Auto	Allows users to set the actual Power Limit value by each individual PoE port.	Auto
Manual	The user can set the power limit value that indicates the power supplied by the system.	

Port Setting

Enable

Setting	Description	Factory Default
Checked	Allows data and power transmission through the port	Enable
Unchecked	Immediately shuts off port access	Enable

Power Limit

Setting	Description	Factory Default
Auto	The amount of power assigned is determined according to the class that is read from the powered device.	Auto
Manual	The user can set the power limit value that indicates the maximum amount of power available to the port.	Auto

The PoE Ethernet switch can monitor PD working status via its IP conditions. If the PD fails, the switch will not receive a PD response after the defined period, and the authentication process is restarted. This is an excellent function to ensure your network reliability and reduce management burden.

PD Failure Check

Setting	Description	Factory Default
Checked	Enables the PD Failure Check function.	Auto
Unchecked	Disables the PD Failure Check function.	Auto

IP

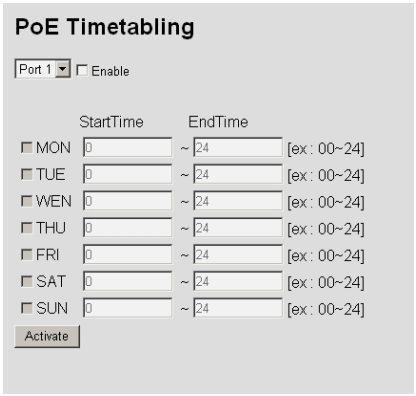
Setting	Description	Factory Default
Max. 15 Characters	Enter the IP for the PD	None

Period

Setting	Description	Factory Default
Max. 5 Characters	Enter the time span for IP checking period	None

3.4.2 PoE Timetabling

Powered devices usually do not need to be running 24 hours a day, 7days a week. The PoE Ethernet switch provides a PoE timetabling mechanism to let users set a flexible working schedule for each PoE port to economize the system's power burden.


PoE Timetabling
Port 1
Enable
StartTime
EndTime
MON 0 ~ 24 [ex : 00~24]
TUE 0 ~ 24 [ex : 00~24]
WEN 0 ~ 24 [ex : 00~24]
THU 0 ~ 24 [ex : 00~24]
FRI 0 ~ 24 [ex : 00~24]
SAT 0 ~ 24 [ex : 00~24]
SUN 0 ~ 24 [ex : 00~24]
Activate

Port

Setting	Description	Factory Default
Port	Enable a dedicated port	Port 1

Enable

Setting	Description	Factory Default
Checked	Enables the port for a defined time period	Disable
Unchecked	Disables the port for a defined time period	

Weekly Timetabling

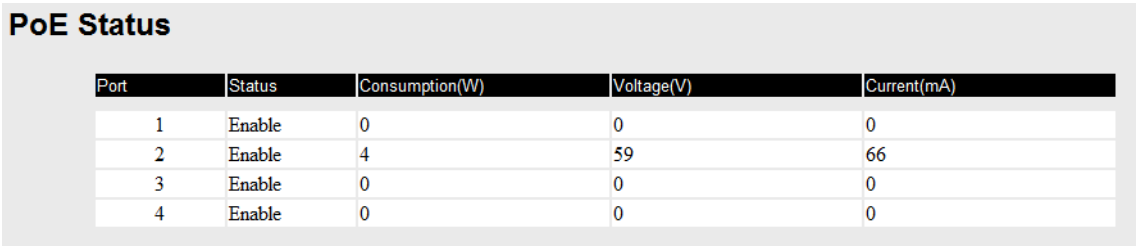
Day

Setting	Description	Factory Default
Checked	Enables the port for a defined number of days	Disable
Unchecked	Disables the port for a defined number of days	

Start/End Time

Setting	Description	Factory Default
Time for working period	Allows users to enter the start and end time for the PD's working period	0-24

3.4.3 PoE Status



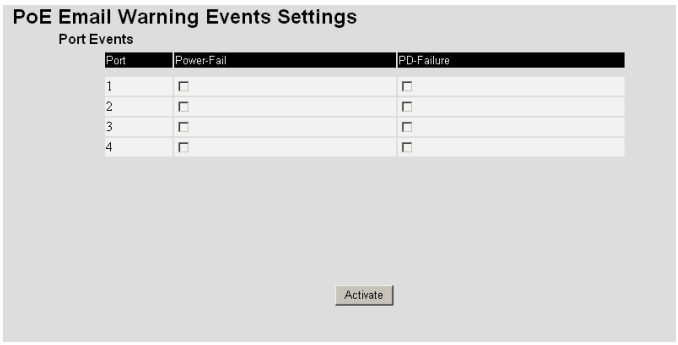
Item	Description
Enable/Disable	Indicates the PoE port status

Consumption (W)	Indicates the actual Power consumed value for PoE port
Voltage (V)	Indicates the actual Voltage consumed value for PoE port
Current (mA)	Indicates the actual Current consumed value for PoE port

3.4.4 PoE Email Warning Events Settings

Since industrial Ethernet devices are often located at the endpoints of a system, these devices do not always know what is happening elsewhere on the network. This means that a PoE port connected to a PD must provide system administrators with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of the PD almost instantaneously when exceptions occur. The PoE Ethernet switch supports different methods for warning engineers automatically, such as email and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms using email and relay output.

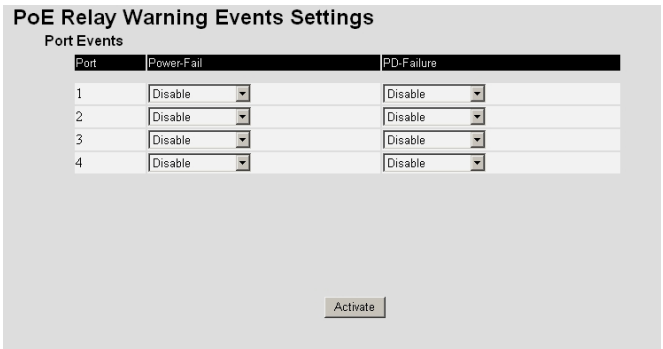
Email Warning Event Types can be divided into two basic groups: Power-Fail and PD-Failure.



Port Events	Warming e-mail is sent when...
Power-Fail	When actual PD power consumption exceeds related PD power limit setting.
PD-Failure	When the switch cannot receive a PD response after the defined period.

3.4.5 PoE Relay Warning Events Settings

Relay Warning Event Types can be divided into two basic groups: Power-Fail and PD-Failure.



Port Events	Warning e-mail is sent when...
Power-Fail	When actual PD power consumption exceeds related PD power limit settings.
PD-Failure	When the switch cannot receive a PD response after the defined period.

3.5 Communication redundancy

3.5.1 Introduction to Communication Redundancy

Setting up Communication Redundancy on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum.

Communication Redundancy allows you to set up *redundant loops* in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable. For example, if the Weidmüller switch is used as a key communications component of a production line, several minutes of downtime could cause a big loss in production and revenue. The Weidmüller switch supports following different protocols for communication redundancy:

- Turbo Ring (V1, original version)
- Turbo Ring V2 (new version with higher performance)
- Turbo Chain
- RSTP (Rapid Spanning Tree) and STP (Spanning Tree Protocols) according to IEEE 802.1W/802.1D-2004

When configuring a redundant ring, all switches on the same ring must be configured to use the same redundancy protocol. You cannot mix the Turbo Ring (V1), Turbo Ring V2, and STP/RSTP protocols on the same ring. The following table lists the key differences between the features of each protocol. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network.

	Turbo Ring V1	**Turbo Ring V2**	**Turbo Chain**	**STP**	**RSTP**
Topology	Ring	Ring	Chain	Ring, Mesh	Ring, Mesh
Recovery Time	< 300 ms	< 20 ms	< 20 ms	Up to 30 sec.	Up to 5 sec

All of Weidmüller's managed switches support following proprietary redundancy protocols:

Turbo Ring (V1) refers to the original version of redundant ring protocol, which has a recovery time of under 300 ms.

Turbo Ring V2 refers to the new generation Turbo Ring, which has a recovery time of under 20 ms. When using ring segments with Gigabit copper interfaces the recovery time is < 50 ms due to a different ring health check method compared to Fast Ethernet interfaces.

Turbo Chain is a redundancy protocol with unlimited flexibility that allows you to construct any type of redundant network topology. The recovery time is under 20 ms.

In this manual, we use the terminology **Turbo Ring** (V1) and **Turbo Ring V2** to differentiate between rings configured for one or the other of these protocols.

Note: By factory default no redundancy protocol is activated.

By factory default the redundancy protocol RSTP generally is selected, but all Switch ports are disabled for beeing a RSTP port.

Note: Port trunking and Turbo Ring can be enabled simultaneously to form a backbone. Doing so will increase the bandwidth of the backbone, and also provide redundancy. For example, suppose that two physical ports, 1 and 2, are trunked to form trunk group Trk1, and then Trk1 is set as one Turbo Ring path. If eg. port 1 gets disconnected, the remaining trunked port 2 will share the traffic. If both ports 1 and 2 gets disconnected, then Turbo Ring automatically is activating the backup path.

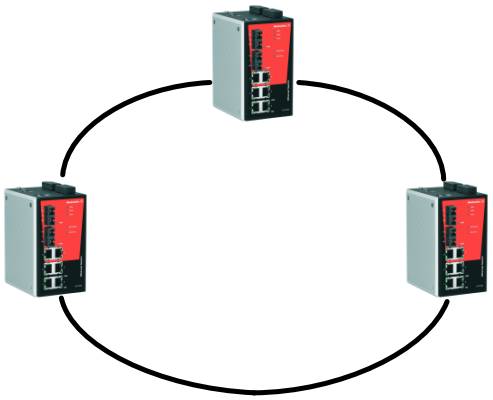
3.5.2 The Turbo Ring Concept

With the proprietaryTurbo Ring protocol you can optimize communication redundancy and achieve a faster recovery time on the network.

The switches have implemented 2 versions of ring redundancy the old version Turbo Ring (V1) and the new version Turbo Ring V2

Both versions of Turbo Ring protocol, original Turbo Ring (V1) and new Turbo Ring V2, identifies one switch as the ***master*** of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically re-adjusts the ring so that the part of the network that was disconnected can re-establish the contact with the rest of the network.

3.5.2.1 Topology Setup for "Turbo Ring (V1)" or "Turbo Ring V2"

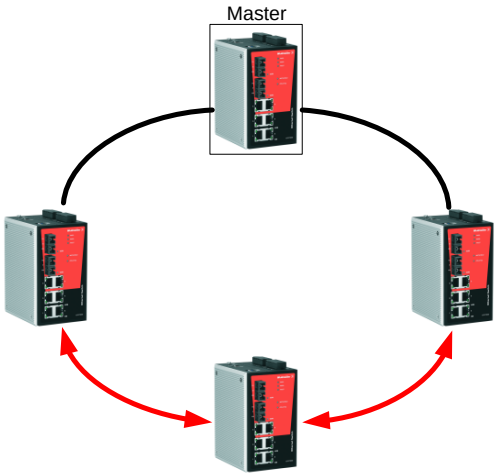
Initial setup of a "Turbo Ring (V1)" or "Turbo Ring V2" ring	
	1. For each switch in the ring, select any two ports as the redundant ports. 2. Connect redundant ports on neighboring switches to form the redundant ring.

When configuring Turbo Ring (both versions) a user does not need to configure any of the switches explicitly as master. If none of the switches in the ring is configured as the master, then the protocol will automatically assign master status to one of the switches. In fact, the master is only used to identify which segment in the redundant ring acts as the backup path. In the following subsections, we explain how the redundant path is selected for rings configured for Turbo Ring (V1) and Turbo Ring V2.

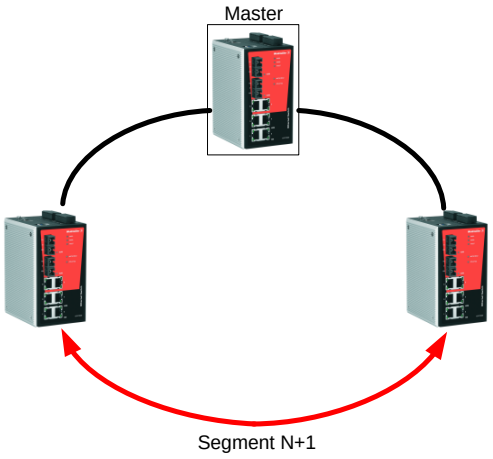
Determining the Redundant Path of a "Turbo Ring"

In this case, the redundant segment (i.e., the segment that will be blocked during normal operation) is determined by the number of switches in the ring, and where the ring master is located.

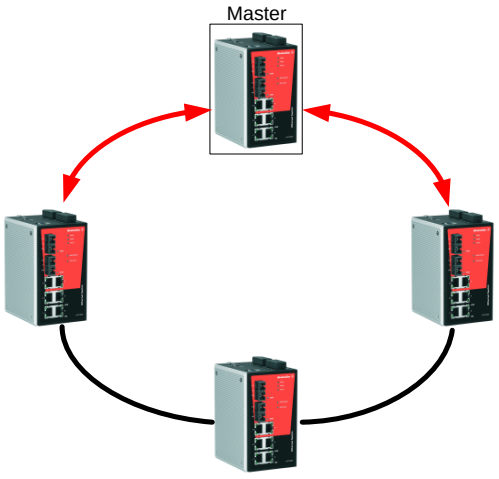
When the Number of Switches in the Turbo Ring (V1) is Even

"Turbo Ring (V1)" with an even number of switches	
	If there are 2N switches (an even number) in the "Turbo Ring", then the backup segment is one of the two segments connected to the (N+1) st switch (i.e., the switch unit directly opposite the master).

When the Number of Switches in the Turbo Ring (V1) is Odd

"Turbo Ring (V1)" with an odd number of switches	
	If there are 2N+switches (an odd number) in the "Turbo Ring", with switches and segments labeled counterclockwise, then segment N+1 will serve as the backup path. For the example shown here, N=1, so that N+1=2.

Turbo Ring V2

Determining the Redundant Path of a "Turbo Ring V2"	
	For a "Turbo Ring V2", the backup segment is the segment connected to the 2nd redundant port on the master. See Configuring "Turbo Ring V2" in the Configuring "Turbo Ring (V1)" and "Turbo Ring V2" section below.

3.5.2.2 Ring Coupling Configuration

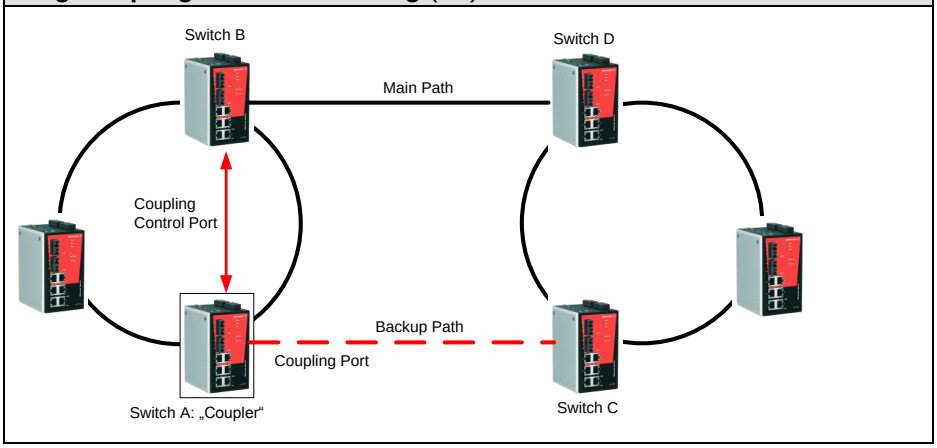
In some applicaions it may not be convenient to connect all devices in the system to form one large redundant ring, though some devices are located in a remote area. For these systems, "**Ring Coupling"** can be used to separate the devices into different smaller redundant rings, but in such a way that they can still communicate with each other.

ATTENTION

In a VLAN environment, the user must set "**Redundant Port"**, "**Coupling Port"**, and "**Coupling Control Port"** to join all VLANs, since these ports act as the *backbone* to transmit all packets of different VLANs to different switches.

Ring coupling based on protocol Turbo Ring (V1, original version)

Ring Coupling for a "Turbo Ring (V1)**"**

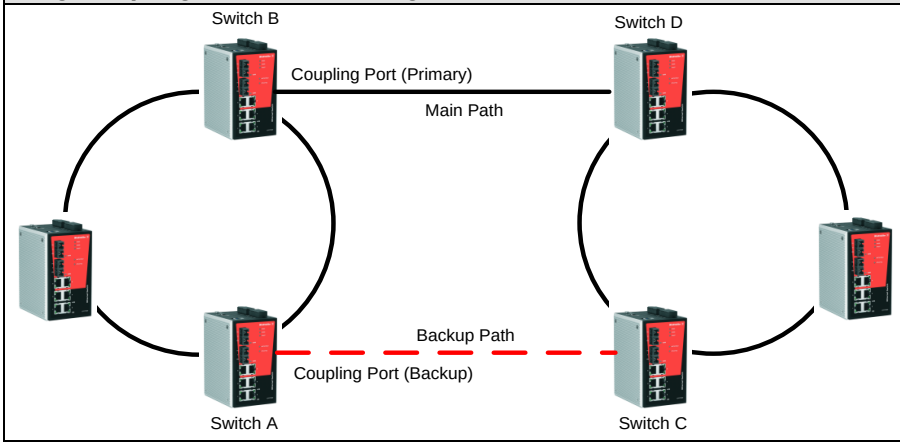


To configure the Ring Coupling function for a **"**Turbo Ring**"**, select two switches (e.g., Switch A and B in the above figure) in the ring, and another two switches in the adjacent ring (e.g., Switch C and D). Decide which two ports in each switch are appropriate to be used as coupling ports, and then link them together. Next, assign one switch (e.g., Switch A) to be the "**coupler"** and connect the coupler's coupling control port with Switch B (for this example).

The coupler switch (i.e., Switch A) will monitor switch B through the coupling control port to determine whether or not the coupling port's backup path should be recovered.

Ring coupling based on protocol Turbo Ring V2 (new version)

Ring Coupling for a "Turbo Ring V2"



Note that the ring coupling settings for a “Turbo Ring V2” are different from a “Turbo Ring”. For Turbo Ring V2, Ring Coupling is enabled by configuring the “**Coupling Port” (Primary)** on Switch B, and the **“Coupling Port” (Backup)** on Switch A only. You do not need to set up a coupling control port, so that a “Turbo Ring V2” does not use a coupling control line.

The “**Coupling Port” (Backup)** on Switch A is used for the backup path, and connects directly to an extra network port on Switch C. The “**Coupling Port” (Primary)** on Switch B monitors the status of the main path, and connects directly to an extra network port on Switch D. With ring coupling established, Switch A can activate the backup path as soon as it detects a problem with the main path.

ATTENTION

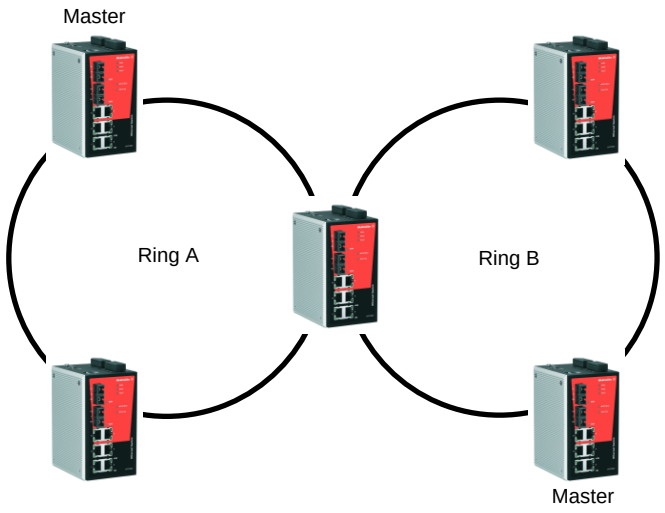
Ring Coupling only needs to be enabled on one of the switches serving as the Ring Coupler. The Coupler must designate different ports as the two Turbo Ring ports and the coupling port.

NOTE: You do not need to use the same Ethernet Switch for both Ring Coupling and Ring Master.

3.5.2.3 Dual-Ring Configuration (applies only to “Turbo Ring V2”)

The “**dual-ring”** option provides another ring coupling configuration, in which two adjacent rings share one switch. This type of configuration is ideal for applications that have inherent cabling difficulties.

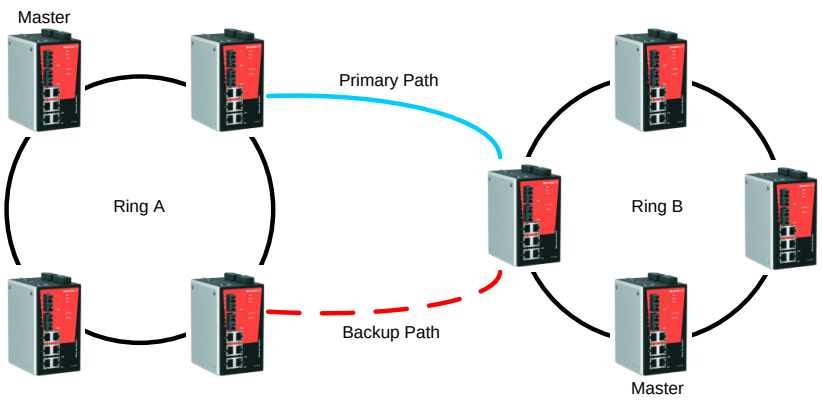
Dual-Ring for a "Turbo Ring V2"



3.5.2.4 Dual-Homing Configuration (applies only to “Turbo Ring V2”)

The “**dual-homing”** option uses a single Ethernet switch to connect two networks. The primary path is the operating connection, and the backup path is a back-up connection that is activated in the event that the primary path connection fails.

Dual-Homing for a "Turbo Ring V2"



3.5.3 Configuring “Turbo Ring (V1)” and “Turbo Ring V2”

Use the **Communication Redundancy** page to select “**Turbo Ring** (V1)**”**, “**Turbo Ring V2”**, or **“Turbo Chain”**. Note that configuration pages for these three protocols are different.

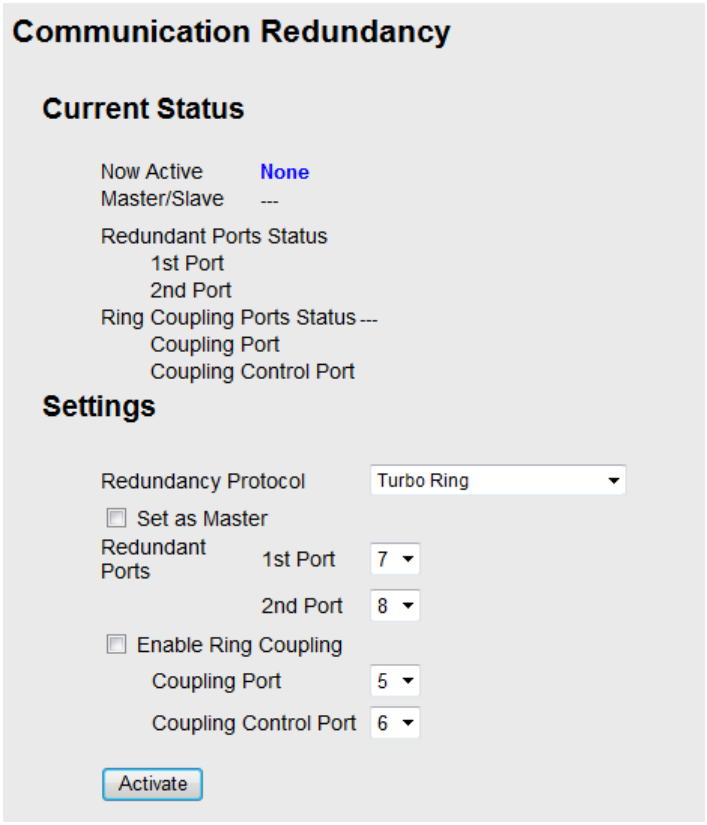
3.5.3.1 Configuring Turbo Ring (V1, original version)

1. Select **Turbo Ring** in field **Redundancy protocol.**

2. Activate checkbox ‘*Set as Master’* for the switch which shall be assigned as ring master.

3. Select the *‘Redundant ports’* which shall be used for the ring.

4. Optionally enable *‘Ring Coupling’* and select coupling ports if a ring coupling topology shall be used.



Explanation of "Current Status" Items

Now Active

It shows which communication protocol is in use: **RSTP**, **Turbo Ring**(V1), **Turbo Ring V2**, **Turbo Chain** or **none**.

Master/Slave

It indicates whether this switch is the Master (or not) of the Turbo Ring. This field appears only when Turbo Ring or Turbo Ring V2 modes are selected.

NOTE: The user does not need to set the master to use Turbo Ring. If master is not set, the Turbo Ring protocol will assign master status to one of the switches in the ring. The master is only used to determine which segment serves as the backup path.

Redundant Ports Status (1st Port, 2nd Port) and

Ring Coupling Ports Status (Coupling Port, Coupling Control Port)

The "Ports Status" indicators show "**Forwarding"** for normal transmission, ***"*Blocking"** if this port is connected to a backup path and the path is blocked, and ***"*Link down"** if there is no connection.

Explanation of *'Setting'* items for selected redundancy protocol Turbo Ring

Set as Master

Setting	Description	Factory Default
Enabled	Select this switch as Master	Not checked
Disabled	Do not select this switch as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the switch to be one of the redundant ports.	See the following table
2nd Port	Select any port of the switch to be one of the redundant ports.	See the following table

Below table lists the **default redundancy ports** dependent on the used models.

Model	Default 1st Port	Default 2nd Port
IE-SW-VL05M/08M Series IE-SW-PL06M/08M/09M/16M Series	The second from the last port of the Switch	The last port of the Switch (highest port number)
IE-SW-PL18M Series	Port G1	Port G2
IE-SW-PL10M Series	Port G2	Port G3

Enable Ring Coupling

Setting	Description	Factory Default
Enable	Select this switch as Coupler	Not checked
Disable	Do not select this switch as Coupler	

Coupling Port

Setting	Description	Factory Default
Coupling Port	Select any port of the switch to be the coupling port	See the following table

Coupling Control Port

Setting	Description	Factory Default
Coupling Control Port	Select any port of the switch to be the coupling control port	See the following table

Below table lists the **default coupling ports** dependent on the used models.

Model	Default Coupling Port	Default Coupling Control Port
IE-SW-VL05M/08M Series IE-SW-PL06M/08M/16M Series	The fourth from the last port of the Switch	The third from the last port (highest port number) of the Switch
IE-SW-PL09M Series	Port G7	Port G6
IE-SW-PL18M Series	Port 15	Port 16
IE-SW-PL10M Series	Port 7	Port G1

3.5.3.2 Configuring Turbo Ring V2 (new version)

1. Select **Turbo Ring V2** in field **Redundancy protocol.**

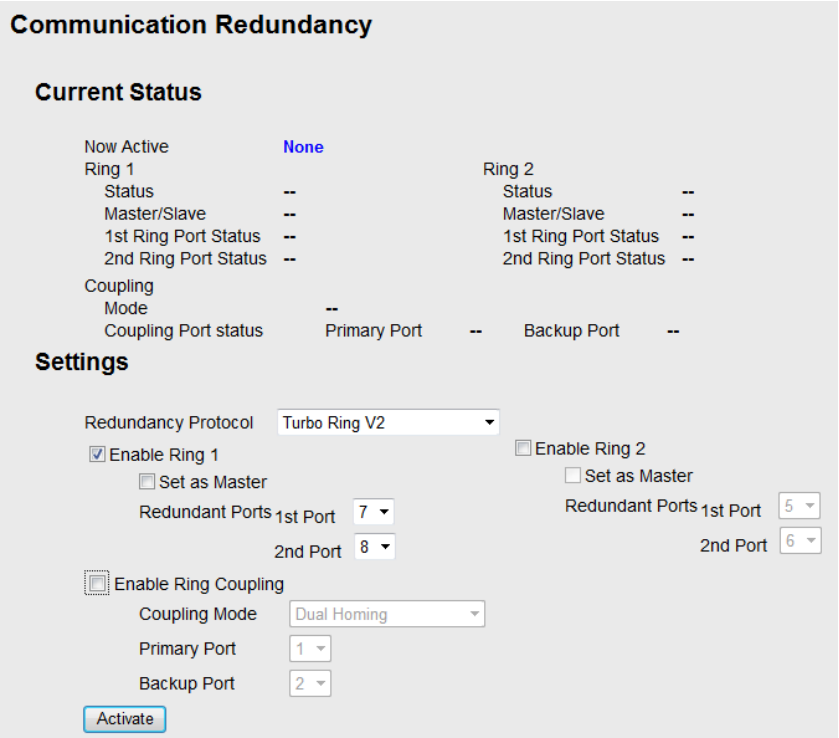
2. If only a redundancy with 1 ring shall be created then do following:

- Activate checkbox '*Enable Ring 1'*
- Activate checkbox '*Set as Master'* (for ring 1) if the switch shall be assigned as ring master for ring 1
- Select the *'Redundant ports'* which shall be used for ring 1

3. If the switch is used to connect 2 Turbo rings (Topology Dual-Ring) then additionally do following:

- Activate checkbox '*Enable Ring 2'*
- Activate checkbox '*Set as Master'* (for ring 2) if the switch shall be assigned as ring master for ring 2
- Select the *'Redundant ports'* which shall be used for ring 2

4. Optionally enable *'Ring Coupling'* and select coupling ports if a ring coupling topology shall be used.



NOTE: When using the Dual-Ring architecture, users must configure settings for both Ring 1 and Ring 2. In this case, the status of both rings will appear under “Current Status.”

Explanation of “Current Status” Items

Now Active

It shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **Turbo Chain, RSTP**, or **none**.

Ring 1/2—Status

It shows **Healthy** if the ring is operating normally, and shows **Break** if the ring’s backup link is active.

Ring 1/2—Master/Slave

It indicates whether this switch is the Master (or not) of the Turbo Ring. This field appears only when Turbo Ring or Turbo Ring V2 modes are selected.

NOTE: The user does not need to set the master to use Turbo Ring. If master is not set, the Turbo Ring protocol will assign master status to one of the Switch units in the ring. The master is only used to determine which segment serves as the backup path.

Ring 1/2—1st/2nd Ring Port Status

The “Ports Status” indicators show ***Forwarding*** for normal transmission, ***Blocking*** if this port is connected to a backup path and the path is blocked, and ***Link down*** if there is no connection.

Coupling—Mode

It indicates either **None**, **Dual Homing** or **Ring Coupling**.

Coupling—Coupling Port status

It indicates either **Primary Port status** or **Backup Port status**.

Explanation of *'Setting'* items for selected redundancy protocol Turbo Ring V2

Enable Ring 1

Setting	Description	Factory Default
Enabled	Enable the Ring 1 settings	checked
Disabled	Disable the Ring 1 settings	Not checked

Enable Ring 2

Setting	Description	Factory Default
Enabled	Enable the Ring 2 settings	Not checked
Disabled	Disable the Ring 2 settings	

Set as Master

Setting	Description	Factory Default
Enabled	Select this Switch as Master	Not checked
Disabled	Do not select this Switch as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the Switch to be one of the redundant ports.	See the following table
2nd Port	Select any port of the Switch to be one of the redundant ports.	See the following table

Below table lists the **default redundancy ports for Ring 1** dependent on the used models.

Model	Default 1st Port	Default 2nd Port
IE-SW-VL05M/08M Series IE-SW-PL06M/08M/09M/16M Series	The second port from the last port number	The last port of the switch (highest port number)
IE-SW-PL18M Series	Port G1	Port G2
IE-SW-PL10M Series	Port G2	Port G3

Below table lists the **default redundancy ports for Ring 2** dependent on the used models

Model	Default 1st Port	Default 2nd Port
IE-SW-VL05M/08M Series IE-SW-PL06M/08M/16M Series	The fourth port from the last port number	The third port from the last port number of the switch
IE-SW-PL09M Series	Port G7	Port G6
IE-SW-PL18M Series	Port 15	Port 16
IE-SW-PL10M Series	Port G1	Port 7

Enable Ring Coupling

Setting	Description	Factory Default
Enable	Select this Switch as Coupler	Not checked
Disable	Do not select this Switch as Coupler	

Coupling Mode

Setting	Description	Factory Default
Dual Homing	Select this item to change to the Dual Homing configuration page	See the following table
Ring Coupling	Select this item to change to the Ring Coupling (backup)	See the following

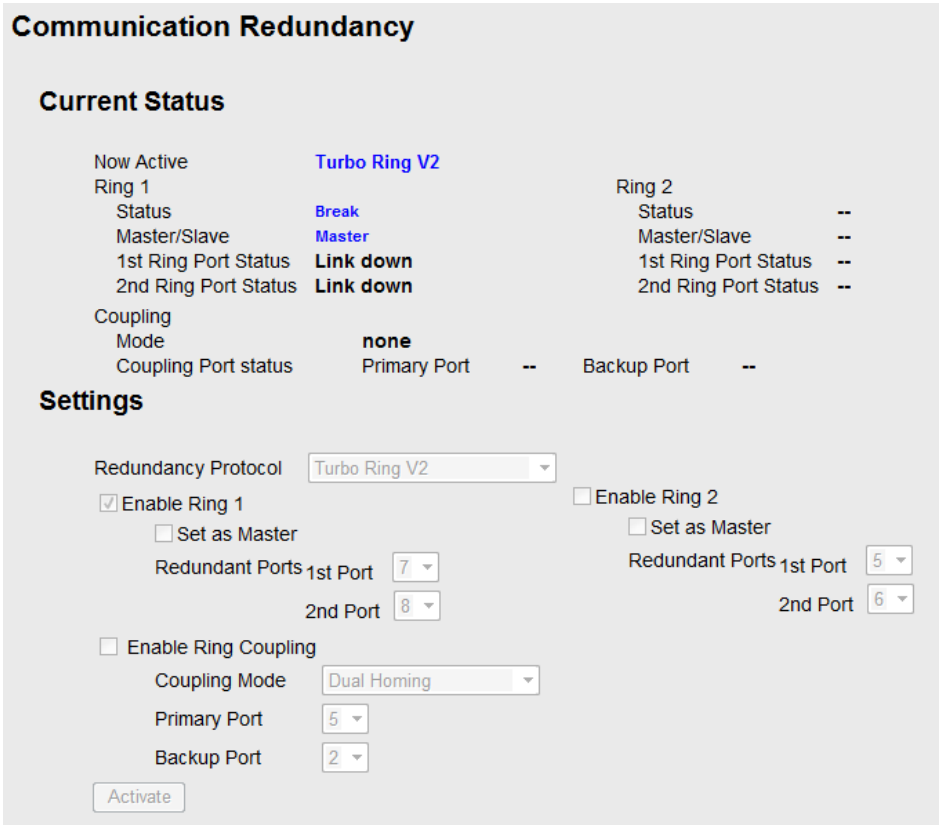
(backup)	configuration page	table
Ring Coupling (primary)	Select this item to change to the Ring Coupling (primary) configuration page	See the following table

Below table lists the **default coupling ports** dependent on the used models.

Model	Default Dual Homing (Primary)	Default Dual Homing (Backup)
All models	Port 1	Port 2

NOTE: The Turbo Ring DIP switches, located on top of the housing, alternatively can be used to configure the Turbo Ring protocols.

If you use the web interface, console interface, or Telnet interface to enable the Turbo Ring DIP Switches, and then set DIP Switch 4 on the switch's outer casing to the **ON** position, you will not be able to use the web interface, console interface, or Telnet interface to change the status of the DIP Switch. In this case, the Communication Redundancy settings will be grayed out in the web browser.



3.5.4 The Turbo Chain Concept

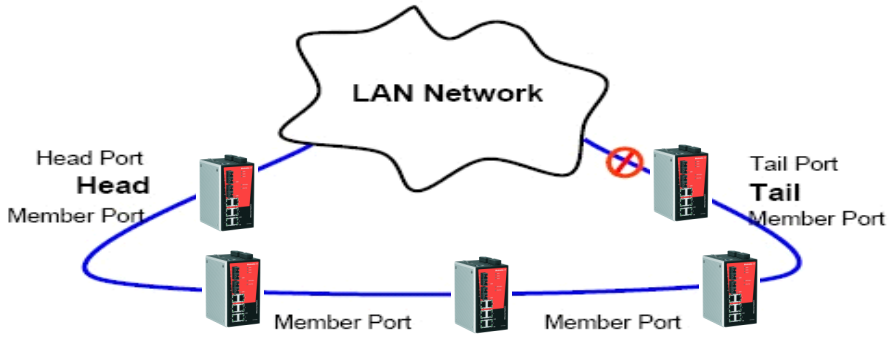
Turbo Chain is an advanced software-technology that gives network administrators the flexibility of constructing any type of redundant network topology. When using the “Turbo Chain” concept, you first connect the Ethernet switches in a chain and then simply link the two ends of the chain to an Ethernet network, as illustrated in the following figure.

Turbo Chain can be used on industrial networks that have a complex topology. If the industrial network uses a multi-ring architecture, Turbo Chain can be used to create flexible and scalable topologies with a fast media-recovery time.

How Turbo Chain generally works

- The Switches are connected as a daisy Chain to any other network
- Chain consists of one header switch (Head), any number of member switches (Member) and one end switch (tail)
- The configured head-port of header switch and configured tail-port of tail are connected to an existing network
- Tail switch blocks its redundancy line (prevent frame looping) and opens only when the main line on head-switch is broken. The healing time inside the Turbo Chain is below 20 ms

Set Up Turbo Chain



3.5.5 Configuring “Turbo Chain”

How to configure Turbo Chain generally:

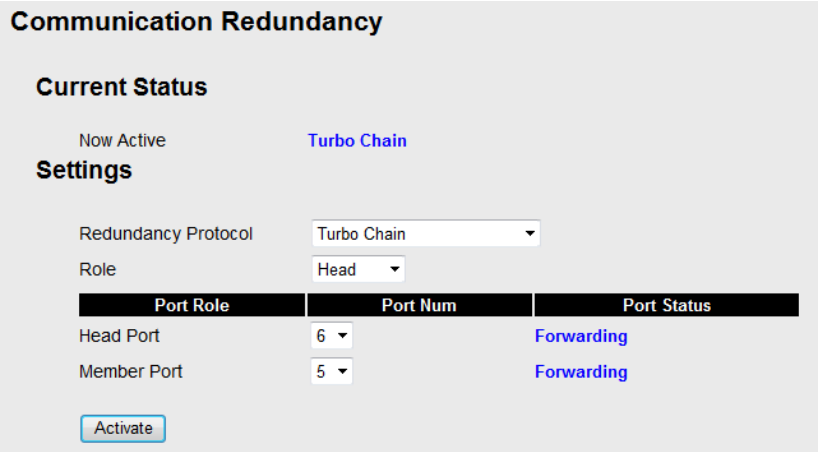
1. Determine which switch shall be used as Head switch, asTail switch and which devices will become Member switches.
2. Configure at Header Switch one port as Head port and one port as Member port.
3. Configure at Tail Switch one port as Tail port and one port as Member port.
4. Configure at all Member Switches two ports as Member ports.
5. Connect the Head switch, Tail switch and Member switches as shown in the diagram.

The connecting path from Head port to the network which shall be attached is the main path and the connecting path to the Tail port is the backup path of the Turbo Chain. Under normal conditions,

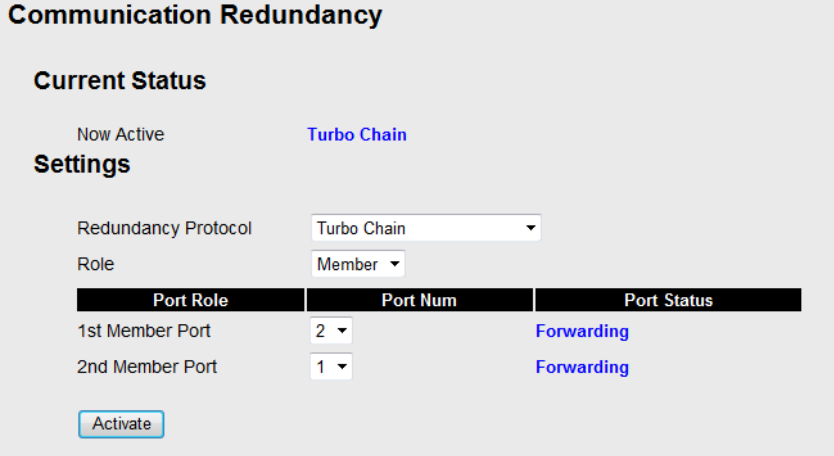
packets are transmitted through the Head Port to the attached network. If any Turbo Chain path is disconnected, the Tail Port will be activated so that packet transmission can continue.

There is no need to change anything in the configuration of the network on which the Turbo Chain switches will be attached.

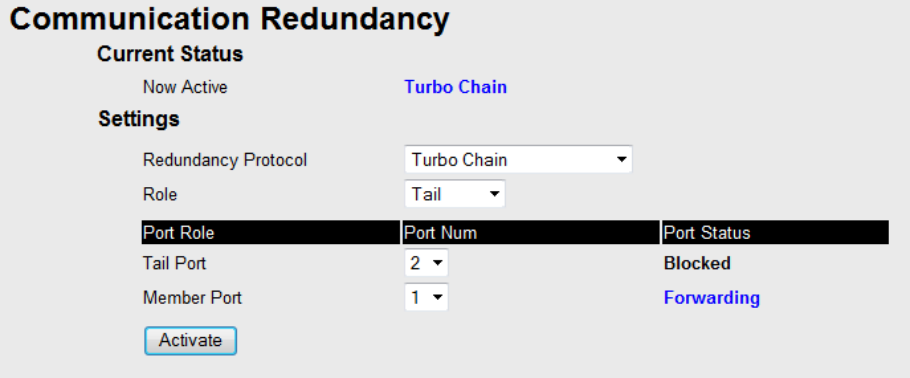
3.5.5.1 Head Switch Configuration



3.5.5.2 Member Switch Configuration



3.5.5.3 Tail Switch Configuration



Explanation of "Current Status" Item

Now Active

It shows which communication protocol is in use: **Turbo Ring V1**, **Turbo Ring V2**, **RSTP**, **Turbo Chain**, or **None**.

The "Ports Status" indicators show ***Forwarding*** for normal transmission, ***Blocked*** if this port is connected to the Tail port as a backup path and the path is blocked, and ***Link down*** if there is no connection.

Explanation of *'Settings'* items for selected redundancy protocol Turbo Chain

Role

Setting	Description	Factory Default
Head	Select this switch as Head Switch	Member
Member	Select this switch as Member Switch	
Tail	Select this switch as Tail Switch	

Head Role (when selected as Head switch)

Setting	Description	Factory Default
Head Port	Select any port of the Switch to be the head port.	See the following table
Member Port	Select any port of the Switch to be the member port.	See the following table

Member Role (when selected as Member switch)

Setting	Description	Factory Default
1st Member port	Select any port of the Switch to be the 1st member port	See the following table
2nd Member port	Select any port of the Switch to be the 2nd member port	See the following table

Tail Role (when selected as Tail switch)

Setting	Description	Factory Default
Tail Port	Select any port of the Switch to be the tail port.	See the following table
Member Port	Select any port of the Switch to be the member port.	See the following table

Below tables lists the **default redundancy ports used for Turbo Chain** dependent on the used models.

Model used as Head	Default Head Port	Default Member Port
IE-SW-VL05M/08M Series IE-SW-PL06M/08M/09M/16M Series	The second port from the last port number	The last port of the switch (highest port number)
IE-SW-PL18M Series	Port G1	Port G2
IE-SW-PL10M Series	Port G2	Port G3

Model used as Member	Default 1st Member Port	Default 2nd Member Port
IE-SW-VL05M/08M Series IE-SW-PL06M/08M/09M/16M Series	The second port from the last port number	The last port of the switch (highest port number)
IE-SW-PL18M Series	Port G1	Port G2
IE-SW-PL10M Series	Port G2	Port G3

Model used as Tail	Default Tail Port	Default Member Port
IE-SW-VL05M/08M Series IE-SW-PL06M/08M/09M/16M Series	The second port from the last port number	The last port of the switch (highest port number)
IE-SW-PL18M Series	Port G1	Port G2
IE-SW-PL10M Series	Port G2	Port G3

3.5.6 STP / RSTP

3.5.6.1 The STP / RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures on a network, and provide an automatic means of avoiding loops. This is particularly important for networks that have a complicated architecture, since unintended loops in the network can cause broadcast storms. Weidmüller switches' STP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every Weidmüller switch connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE 802.1D-2004. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy.

For example:

- Defaults to sending 802.1D style BPDUs if packets with this format are received.
- STP (802.1D) and RSTP (802.1w) can operate on different ports of the same switch, which is particularly helpful when switch ports connect to older equipment such as legacy switches.

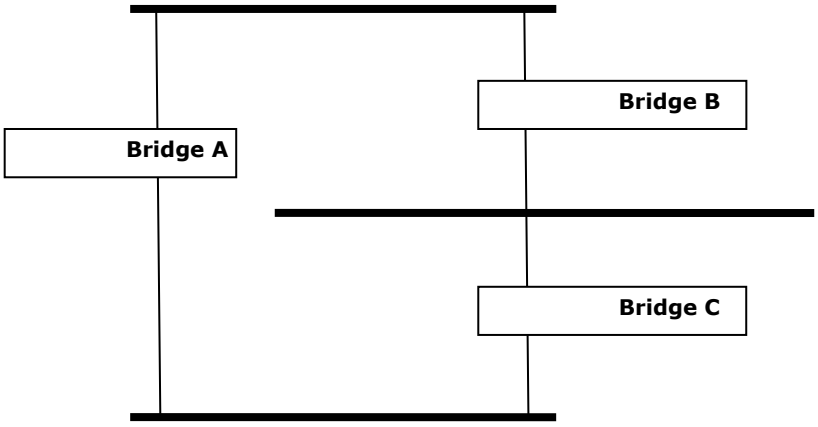
You get essentially the same functionality with RSTP and STP. To see how the two systems differ, see section '*Differences between STP and RSTP*' later in this chapter.

NOTE: The STP protocol is part of the IEEE Std 802.1D, 2004 Edition bridge specification. The following explanation uses "bridge" instead of "switch."

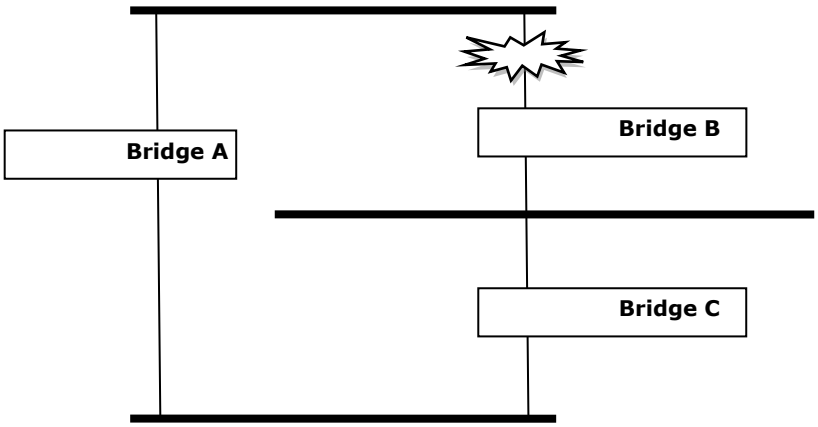
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- Locate and then disable less efficient paths (i.e., paths that have a lower bandwidth).
- Enable one of the less efficient paths if a more efficient path fails.

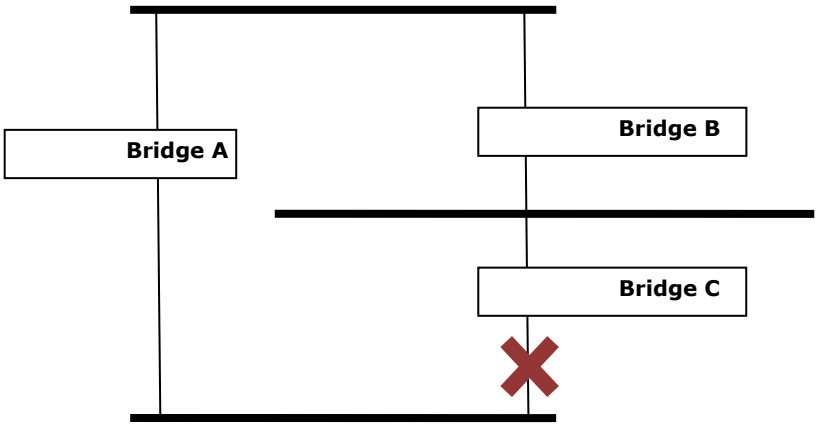
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



If STP is enabled, it will detect duplicate paths and prevent, or *block*, one of the paths from forwarding traffic. In the following example, STP determined that traffic from LAN segment 2 to LAN segment 1 should flow through bridges C and A since this path has a greater bandwidth and is therefore more efficient.



What happens if a link failure is detected? As shown in next figure, the STP process reconfigures the network so that traffic from LAN segment 2 flows through bridge B.



STP will determine which path between each bridged segment is most efficient, and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous 3 figures, STP first determined that the path through bridge C was the most efficient, and as a result, blocked the path through bridge B. After the failure of bridge C, STP re-evaluated the situation and opened the path through Bridge B.

3.5.6.2 How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the sections below.

STP Requirements

Before STP can configure the network, the system must satisfy the following requirements:

- All bridges must be able to communicate with each other. The communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. For example, the default priority setting of Weidmüller switches is 32768.
- Each port has a cost that specifies the efficiency of each link. The efficiency cost is usually determined by the bandwidth of the link, with less efficient links assigned a higher cost. The following table shows the default port costs for a switch:

Port Speed	Path Cost 802.1D, 1998 Edition	Path Cost 802.1w-2001
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1000 Mbps	4	20,000

STP Calculation

The first step of the STP process is to perform calculations. During this stage, each bridge on the network transmits BPDUs. The following items will be calculated:

- Which bridge should be the **Root Bridge**. The Root Bridge is the central reference point from which the network is configured.
- The **Root Path Costs** for each bridge. This is the cost of the paths from each bridge to the Root Bridge.
- The identity of each bridge's **Root Port**. The Root Port is the port on the bridge that connects to the Root Bridge via the most efficient path. In other words, the port connected to the Root Bridge via the path with the lowest Root Path Cost. The Root Bridge, however, does not have a Root Port.
- The identity of the **Designated Bridge** for each LAN segment. The Designated Bridge is the bridge with the lowest Root Path Cost from that segment. If several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge. Traffic

transmitted in the direction of the Root Bridge will flow through the Designated Bridge. The port on this bridge that connects to the segment is called the **Designated Bridge Port**.

STP Configuration

After all of the bridges on the network agree on the identity of the Root Bridge, and all other relevant parameters have been established, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they will not be allowed to receive or forward traffic.

STP Reconfiguration

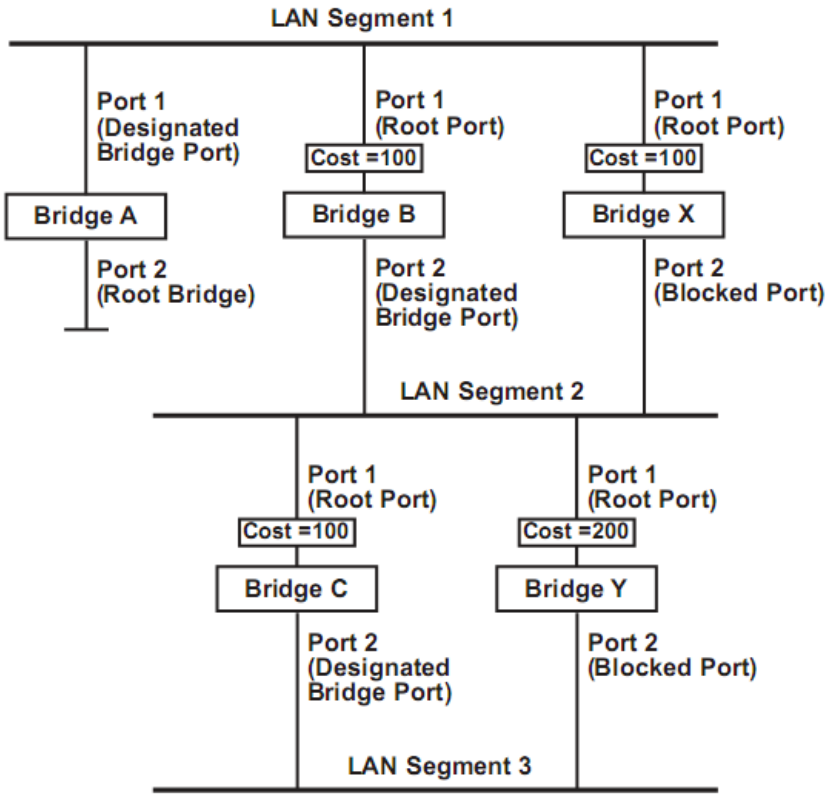
Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has ceased to function. This will trigger the bridge to reconfigure the network to account for the change. If you have configured an SNMP trap destination, when the topology of your network changes, the first bridge to detect the change will send out an SNMP trap.

Differences between STP and RSTP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

STP Example

The LAN shown in the following figure has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.

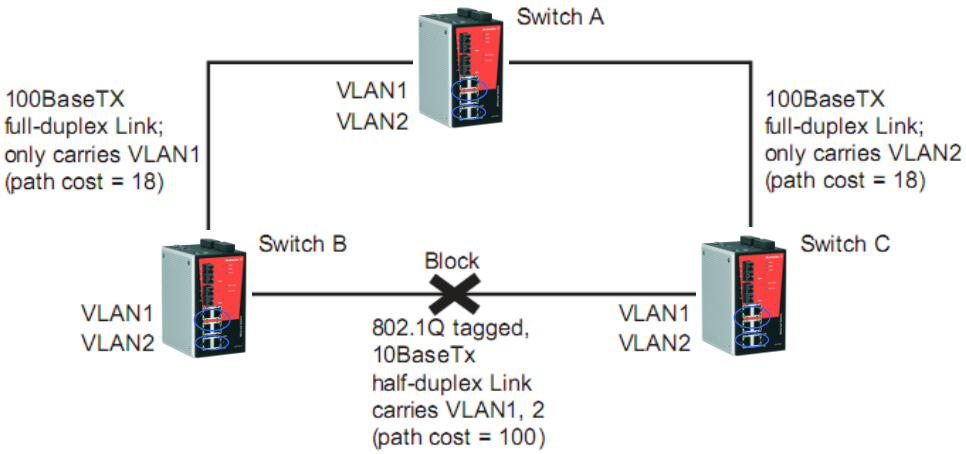


- Bridge A has been selected as the Root Bridge, since it was determined to have the lowest Bridge Identifier on the network.
- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.
- Ports 1 of Bridges B, C, X, and Y are all Root Ports since they are nearest to the Root Bridge, and therefore have the most efficient path.
- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B was selected as the Designated Bridge for that segment since it has a lower Bridge Identifier. Port 2 on Bridge B is selected as the Designated Bridge Port for LAN Segment 2.
- Bridge C is the Designated Bridge for LAN segment 3, because it has the lowest Root Path Cost for LAN Segment 3:
  - The route through bridges C and B costs 200 (C to B=100, B to A=100)
  - The route through bridges Y and B costs 300 (Y to B=200, B to A=100)
- The Designated Bridge Port for LAN Segment 3 is port 2 on bridge C.

Using STP on a Network with Multiple VLANs

IEEE Std 802.1D, 1998 Edition, does not take into account VLANs when calculating STP information—the calculations only depend on the physical connections. Consequently, some network configurations will result in VLANs being subdivided into a number of isolated sections by the STP system. You must ensure that every VLAN configuration on your network takes into account the expected STP topology and alternative topologies that may result from link failures.

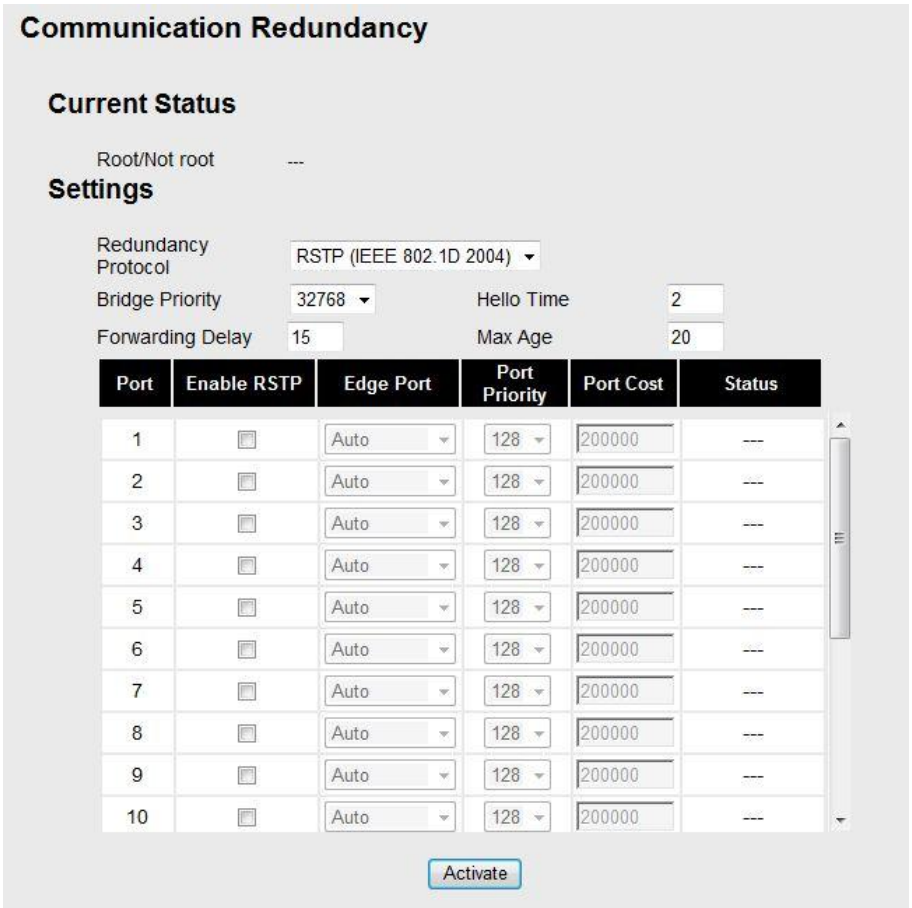
The following figure shows an example of a network that contains VLANs 1 and 2. The VLANs are connected using the 802.1Q-tagged link between switch B and Switch C. By default, this link has a port cost of 100 and is automatically blocked because the other switch-to-switch connections have a port cost of 36 (18+18). This means that both VLANs are now subdivided—VLAN 1 on switches A and B cannot communicate with VLAN 1 on switch C, and VLAN 2 on switches A and C cannot communicate with VLAN 2 on switch B.



To avoid subdividing VLANs, all inter-switch connections should be made members of all available 802.1Q VLANs. This will ensure connectivity at all times. For example, the connections between switches A and B, and between switches A and C, should be 802.1Q tagged and carrying VLANs 1 and 2 to ensure connectivity.

3.5.7 Configuring STP / RSTP

The following figures indicate which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter follows.



At the top of this page, the user can check the **Current Status** of this function. For RSTP, you will see:

Root/Not Root

This field only appears when RSTP mode is selected. The field indicates whether or not this switch is the Root of the Spanning Tree (the root is determined automatically).

At the bottom of this page, the user can configure the "**Settings"** of this function. For RSTP, you can configure:

Explanation of *'Settings'* items for selected redundancy protocol RSTP

Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Forwarding Delay (sec)

Setting	Description	Factory Default
Numerical value input by user	The amount of time this device waits before checking to see if it should change to a different state.	15

Hello time (sec)

Setting	Description	Factory Default
Numerical value input by user	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2

Max. Age (sec)

Setting	Description	Factory Default
Numerical value input by user	If this device is not the root, and it has not received a hello message from the root in an amount of time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20

Enable RSTP per Port

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as a node on the Spanning Tree topology.	Disabled

NOTE: We suggest not enabling the Spanning Tree Protocol once the port is connected to a device (PLC, RTU, etc.) as opposed to network equipment. The reason is that it will cause unnecessary negotiation.

Edge Port

Setting	Description	Factory Default
Auto	1. If the port does not receive a BPDU within 3 seconds, the port will be in the forwarding state. 2. Once the port receives a BPDU, it will start the RSTP negotiation process.	Auto
Force Edge	The port is fixed as an edge port and will always be in the forwarding state	
False	The port is set as the normal RSTP port	

Port Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by entering a lower number.	128

Port Cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology.	200000

Port Status

It indicates the current Spanning Tree status of this port. "**Forwarding"** for normal transmission, or "**Blocking"** to block transmission.

Configuration Limits of STP/RSTP

The Spanning Tree Algorithm places limits on three of the configuration items described previously:

Rule/Limitation 1: 1 sec ≦ Hello Time ≦ 10 sec

Rule/Limitation 2: 6 sec ≦ Max. Age ≦ 40 sec

Rule/Limitation 3: 4 sec ≦ Forwarding Delay ≦ 30 sec

These three variables are further restricted by the following two inequalities:

Rule/Limitation 4: 2 x (Hello Time + 1 sec) ≦ Max. Age ≦ 2 x (Forwarding Delay – 1 sec)

The firmware will alert you immediately if any of these restrictions are violated.

For example, setting Hello Time = 5 sec and
Max. Age = 20 sec and
Forwarding Delay = 4 sec

does not violate rule 1 through 3, but does violate rule 4 because in this case

2 x (Hello Time + 1 sec) = 12 sec and

2 x (Forwarding Delay – 1 sec) = 6 sec.

You can remedy the situation in many ways. One solution is simply to increase the Forwarding Delay value to at least 11 sec.

Perform the following steps to avoid repetitive approach:

Step 1: Assign a value to "**Hello Time"** and then calculate the left most part of rule 4 to get the lower limit of "**Max. Age"**.

Step 2: Assign a value to "**Forwarding Delay"** and then calculate the right most part of rule 4 to get the upper limit for "**Max. Age"**.

Step 3: Assign a value to "**Forwarding Delay"** that satisfies the conditions.

3.6 Using Traffic Prioritization

The Weidmüller switch's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The Weidmüller switch can inspect both IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information to provide consistent classification of the entire network. The implemented QoS capability improves the performance and determinism of industrial networks for mission critical applications.

3.6.1 The Traffic Prioritization Concept

What is Traffic Prioritization?

Traffic prioritization allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- Improve network performance by controlling a wide variety of traffic and managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or business-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP, and minimize traffic delay and jitter.
- Improve network performance as the amount of traffic grows. This will save cost by reducing the need to keep adding bandwidth to the network.

How Traffic Prioritization Works

Traffic prioritization uses the four traffic queues that are present in your Weidmüller managed Switch to ensure that high priority traffic is forwarded on a different queue from lower priority traffic. This is what provides Quality of Service (QoS) to your network.

Weidmüller managed Switch traffic prioritization depends on two industry-standard methods:

- **IEEE 802.1D → A** layer 2 marking scheme.
- **Differentiated Services (DiffServ) → A** layer 3 marking scheme.

IEEE 802.1D Traffic Marking

The IEEE Std 802.1D, 1998 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. The 4-byte tag immediately follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D, 1998 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame. The priority marking scheme determines the level of service that this type of traffic should receive. Refer to the table below for an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority Level	IEEE 802.1D Traffic Type
0	Best Effort (default)
1	Background
2	Standard (spare)
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (interactive media); less than 100 milliseconds of latency and jitter
6	Voice (interactive voice); less than 10 milliseconds of latency and jitter
7	Network Control Reserved traffic

Even though the IEEE 802.1D standard is the most widely used prioritization scheme in the LAN environment, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional for Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.
- It is only supported on a LAN and not across routed WAN links, since the IEEE 802.1Q tags are removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to store the packet priority information. DSCP is an advanced intelligent method of traffic marking that allows you to choose how your network prioritizes different types of traffic. DSCP uses 64 values that map to user-defined service levels, allowing you to establish more control over network traffic.

The advantages of DiffServ over IEEE 802.1D are:

- You can configure how you want your switch to treat selected applications and types of traffic by assigning various grades of network service to them.
- No extra tags are required in the packet.
- DSCP uses the IP header of a packet to preserve priority across the Internet
- DSCP is backward compatible with IPV4 TOS, which allows operation with existing devices that use a layer 3 TOS enabled prioritization scheme.

Traffic Prioritization

Weidmüller managed Switches classify traffic based on layer 2 of the OSI 7 layer model, and the switch prioritizes received traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1D frame and is assigned to the appropriate priority queue based on the IEEE 802.1p service level value defined in that packet. Service level markings (values) are defined in the IEEE 802.1Q 4-byte tag, and consequently traffic will only contain 802.1p priority markings if the network is configured with VLANs and VLAN tagging. The traffic flow through the switch is as follows:

- A packet received by the switch may or may not have an 802.1p tag associated with it. If it does not, then it is given a default 802.1p tag (which is usually 0). Alternatively, the packet may be marked with a new 802.1p value, which will result in all knowledge of the old 802.1p tag being lost.

- As the 802.1p priority levels are fixed to the traffic queues, the packet will be placed in the appropriate priority queue, ready for transmission through the appropriate egress port. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port is tagged for that VLAN. If it is, then the new 802.1p tag is used in the extended 802.1D header.

- The Weidmüller Switch will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based upon the IEEE 802.1p value (service levels) in that tag. It is this 802.1p value that determines to which traffic queue the packet is mapped to.

Traffic Queues

The hardware of Weidmüller switches has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the Weidmüller switch without being delayed by lower priority traffic. As each packet arrives in the Weidmüller switch, it passes through any ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue.

The Weidmüller switches support two different queuing mechanisms:

- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weight Fair method gives high priority precedence over

low priority, but in the event that high priority traffic does not reach the link capacity, lower priority traffic is not blocked.

- **Strict:** This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. The Strict method always gives precedence to high priority over low priority.

3.6.2 Configuring Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization capability to ensure that important data is delivered consistently and predictably. The Weidmüller switch can inspect IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information, to provide a consistent classification of the entire network. The implemented QoS capability improves your industrial network's performance and determinism for mission critical applications.

3.6.2.1 QoS Classification

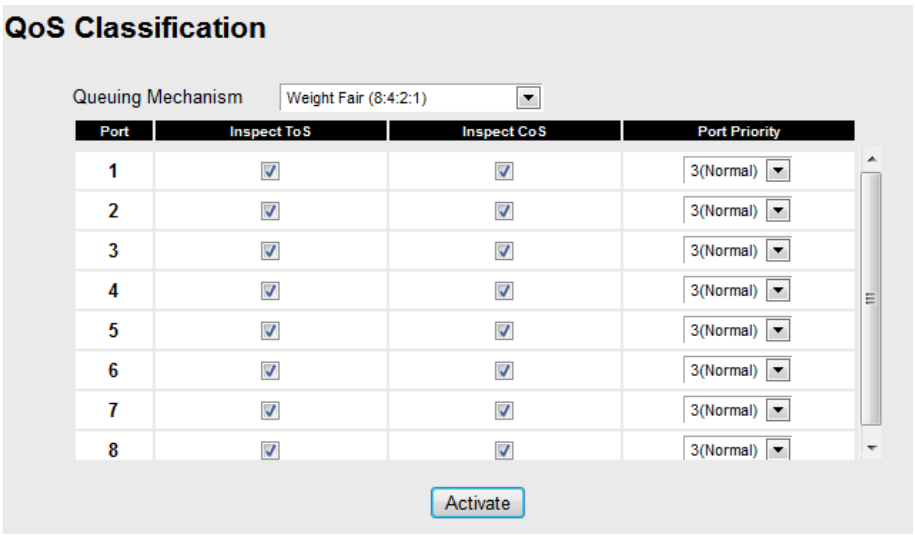
NOTE: Generally the priority of an ingress frame is determined in following order:

1. **Port Priority**
2. **Inspect TOS**
3. **Inspect CoS**

There are two QoS classification settings depending on the specific model of the switch.

Type	Models Supported
Type 1	IE-SW-VL05M/VL08M series, IE-SW-PL06M/PL08M/PL09M/PL10M series
Type 2	IE-SW-PL16M/PL18M series

Type 1 (IE-SW-VL05M/VL08M series, IE-SW-PL06M/PL08M/PL09M/PL10M series)



The Weidmüller switch supports inspection of layer 3 TOS and/or layer 2 CoS tag information to determine how to classify traffic packets.

Queuing Mechanism – Type 1

Setting	Description	Factory Default
Weight Fair	The Weidmüller switch has 4 priority queues. In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

Inspect TOS – Type 1

Setting	Description	Factory Default
Enable/Disable	Enables or disables the Weidmüller switch for inspecting Type of Service (TOS) bits in the IPV4 frame to determine the priority of each frame.	Enabled

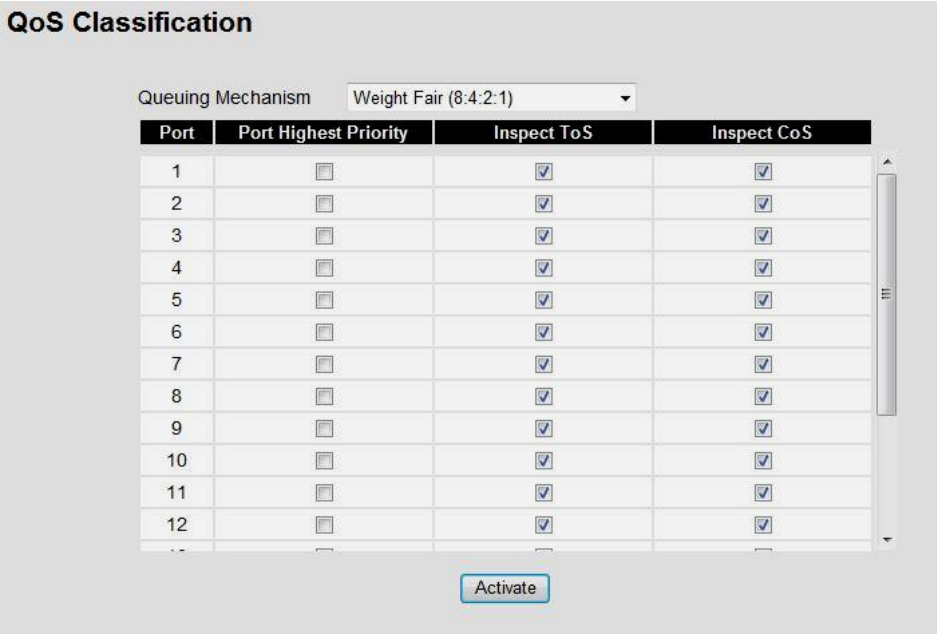
Inspect COS – Type 1

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the Switch to inspect the 802.1p COS tag in the MAC frame to determine the priority of each frame.	Enabled

Port Priority – Type 1

Setting	Description	Factory Default
Port priority	The port priority has 4 priority queues. Low, normal, medium, high priority queue option is applied to each port.	3(Normal)

Type 2 (IE-SW-PL16M/PL18M series)



Queuing Mechanism – Type 2

Setting	Description	Factory Default
Weight Fair	The Weidmüller switch has 4 priority queues. In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

Port Highest Priority – Type 2

Setting	Description	Factory Default
Enable/Disable	Enables or disables the priority inspection of each port	Diabled

Inspect TOS – Type 2

Setting	Description	Factory Default
Enable/Disable	Enables or disables the Weidmüller switch for	Enabled

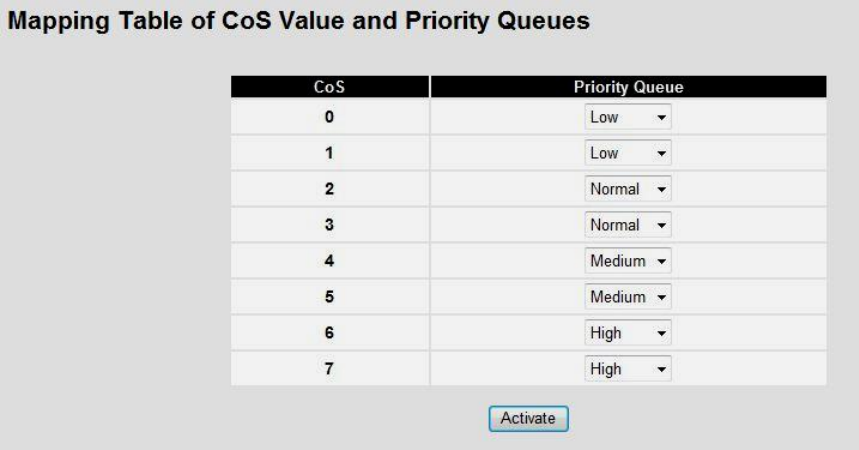
	inspecting Type of Service (TOS) bits in the IPV4 frame to determine the priority of each frame.	

Inspect COS – Type 2

Setting	Description	Factory Default
Enable/Disable	Enables or disables the Weidmüller Switch for inspecting 802.1p COS tags in the MAC frame to determine the priority of each frame.	Enabled

NOTE: The designer can enable these classifications individually or in combination. For instance, if a “hot” higher priority port is required for a network design, “Inspect TOS” and “Inspect CoS” can be disabled. This setting leaves only port default priority active, which results in all ingress frames being assigned the same priority on that port.

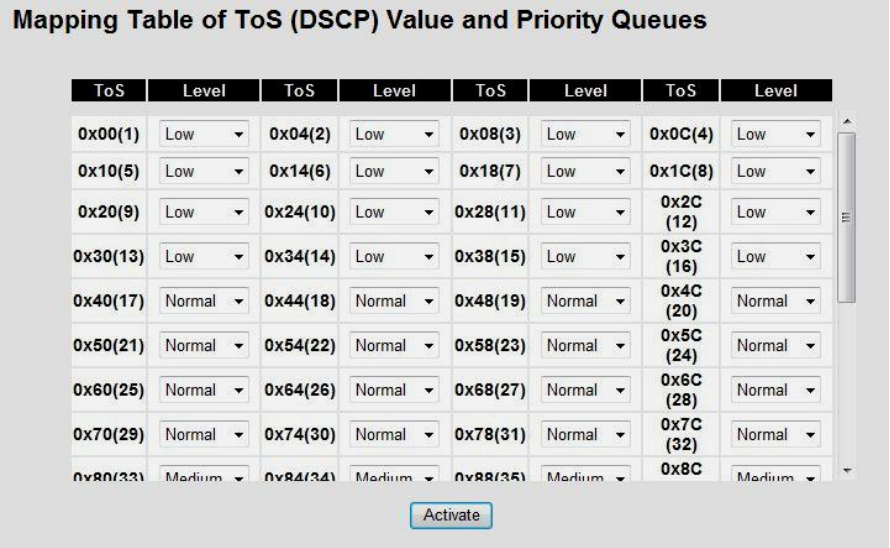
3.6.2.2 CoS Mapping



CoS Value and Priority Queues

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different CoS values to 4 different egress queues.	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

3.6.2.3 ToS/DiffServ Mapping



ToS (DSCP) Value and Priority Queues

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different ToS values to 4 different egress queues..	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

3.7 Using Virtual LAN

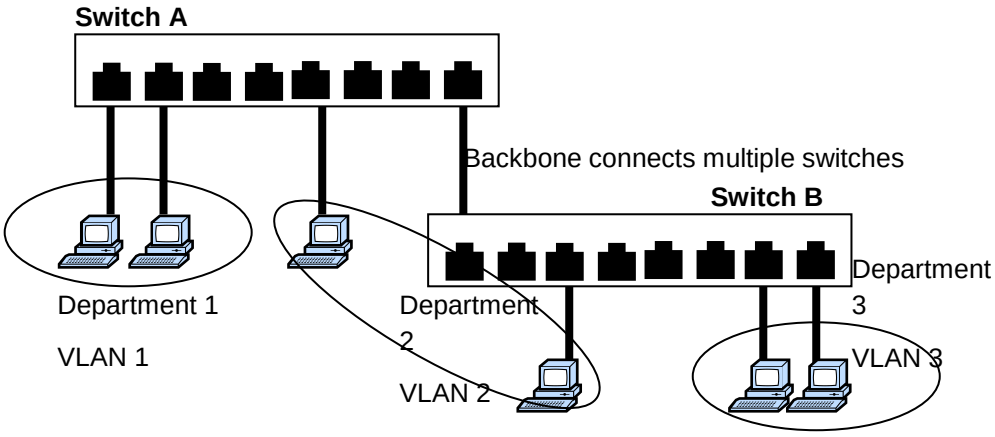
Setting up Virtual LANs (VLANs) on your Weidmüller switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

3.7.1 The Virtual LAN (VLAN) Concept

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. With VLANs you can segment your network according into:

- **Departmental groups**—You could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups**—You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—You could have one VLAN for email users and another for multimedia users.



Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend most of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host on VLAN Marketing, for example, is moved to a port in another part of the network, and retains its original subnet membership, you only need to specify that the new port is on VLAN Marketing. You do not need to carry out any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on VLAN Marketing needs to communicate with devices on VLAN Finance, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs

Your Weidmüller switch provides support for VLANs using IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-1998 standard allows each port on your Weidmüller switch to be placed in:

- On a single VLAN defined in the Weidmüller switch
- On several VLANs simultaneously using 802.1Q tagging

The standard requires that you define the *802.1Q VLAN ID* for each VLAN on your Weidmüller switch before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized Weidmüller contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- *VLAN Name*—Management VLAN
- *802.1Q VLAN ID*—1 (if tagging is required)

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the Weidmüller switch over the network.

Communication between VLANs

If devices connected to a VLAN need to communicate to devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

The Weidmüller switch supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical (backbone, trunk) link. When setting up VLANs you need to understand when to use untagged and tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, tagged membership must be defined.

A typical host (e.g., clients) will be untagged members of one VLAN, defined as "Access Port" in the Weidmüller switch, while inter-switch connections will be tagged members of all VLANs, defined as "Trunk Port" in the Weidmüller switch.

The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs. If a frame is carrying the additional information, it is known as a *tagged* frame.

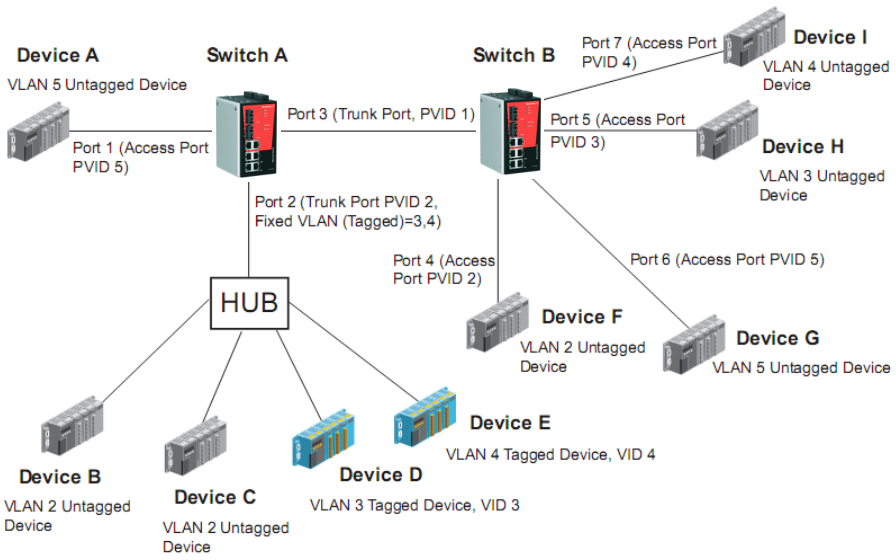
To carry multiple VLANs across a single physical (backbone, trunk) link, each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong to which VLAN. To communicate between VLANs, a router must be used.

The Weidmüller switch supports three types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that assigns which VLAN the device belongs to. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the switch will insert this PVID into this packet so the next 802.1Q VLAN switch can recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices, tagged devices and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign a PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the port default PVID as its VID.
- **Hybrid Port:** The port is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

The following section illustrates how to use these ports to set up different applications.

Sample Applications of VLANs Using Weidmüller Switches



In this application,

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as "Access Port" with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as "Trunk Port" with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port can only belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as "Trunk Port." GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as "Access Port" with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as "Access Port" with PVID 3.
- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as "Access Port" with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as "Access Port" with PVID 4.

After proper configuration:

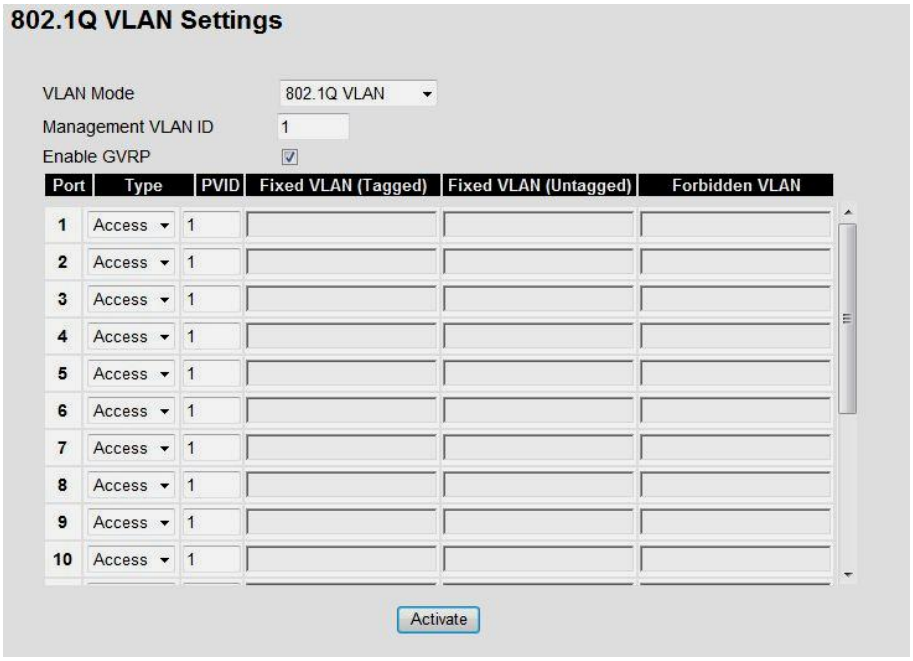
- Packets from device A will travel through "Trunk Port 3" with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by device G, and vice versa.
- Packets from device B and C will travel through "Trunk Port 3" with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by device F, and vice versa.
- Packets from device D will travel through "Trunk Port 3" with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by device H. Packets from device H will travel through "Trunk Port 3" with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device D.
- Packets from device E will travel through "Trunk Port 3" with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by device I. Packets from device I will travel through "Trunk Port 3" with tagged VID 4. Switch A will

recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device E.

3.7.2 Configuring Virtual LAN

3.7.2.1 VLAN Settings

To configure 802.1Q VLAN and port-based VLANs on the Weidmüller switch, use the **VLAN Settings** page to configure the ports.



VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	

Management VLAN ID

Setting	Description	Factory Default
VLAN ID from 1 to 4094	Assigns the VLAN ID of the Weidmüller switch.	1

Port Type

Setting	Description	Factory Default
Access	This port type is used to connect single devices without tags.	Access
Trunk	Select "Trunk" port type to connect another 802.1Q VLAN aware switch.	
Hybrid	Select Hybrid port to connect another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs.	

ATTENTION

For communication redundancy in the VLAN environment, set **Redundant Port**, **Coupling Port**, and **Coupling Control Port** as "Trunk Port," since these ports act as the "backbone" to transmit all packets of different VLANs to different Weidmüller switches.

Port PVID

Setting	Description	Factory Default
VID ranges from 1 to 4094	Sets the default VLAN ID for untagged devices that connect to the port.	1

Fixed VLAN (Tagged)

Setting	Description	Factory Default
VID ranges from 1 to 4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	None

Fixed VLAN List (Untagged)

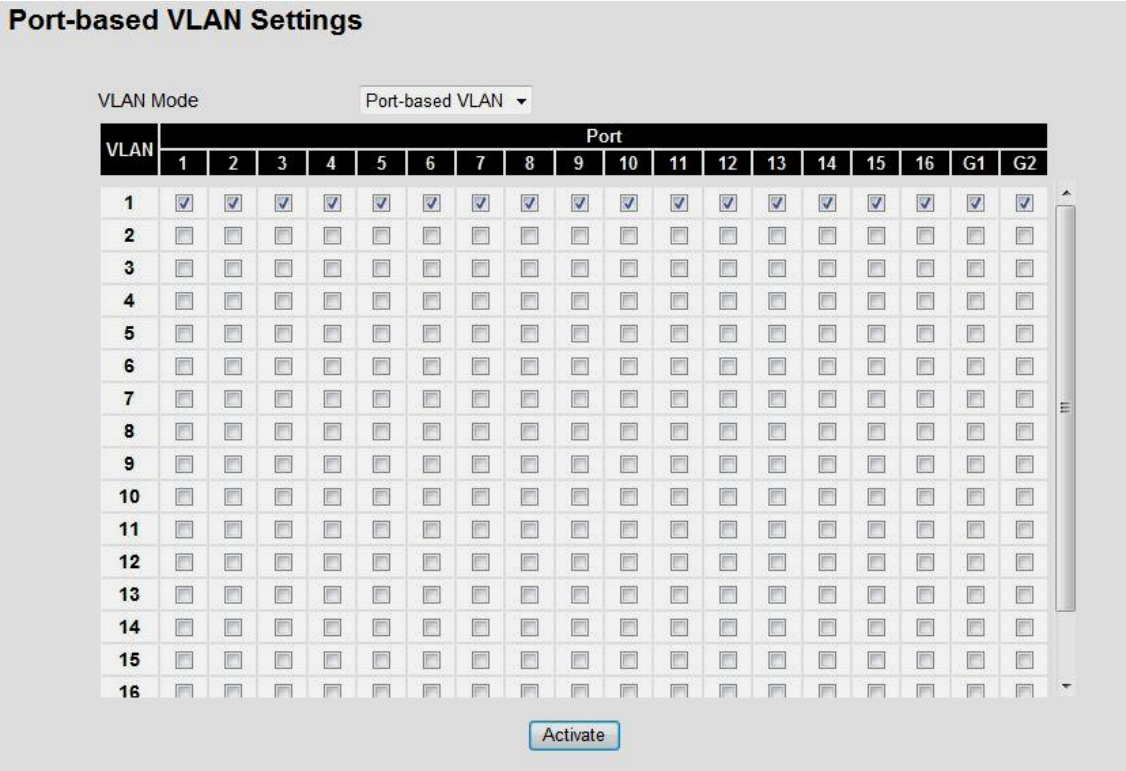
Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the Hybrid port type. Set the VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	None

Forbidden VLAN List

Setting	Description	Factory Default
VID ranges from 1 to 4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the VLAN IDs that will not be supported by this trunk port. Use commas to separate different VIDs.	None

3.7.2.2 Port-Based VLAN Settings

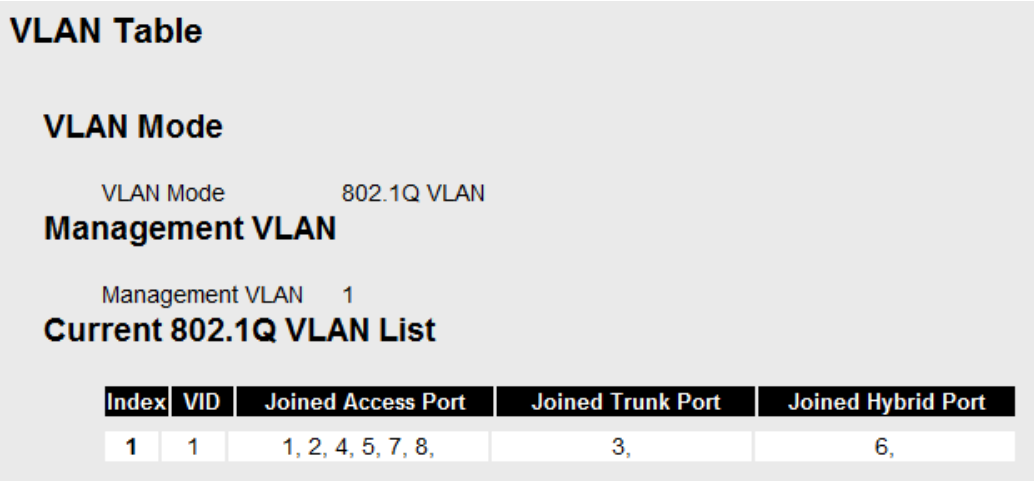
Check each specific port to assign its VLAN ID in the table. The maximum VLAN ID is the same as your number of switch ports.



Port

Setting	Description	Factory Default
Enable/Disable	Set port to specific VLAN Group by activating checkbox.	Enable (all ports belong to VLAN1)

3.7.2.3 VLAN Table



VLAN Table

VLAN Mode

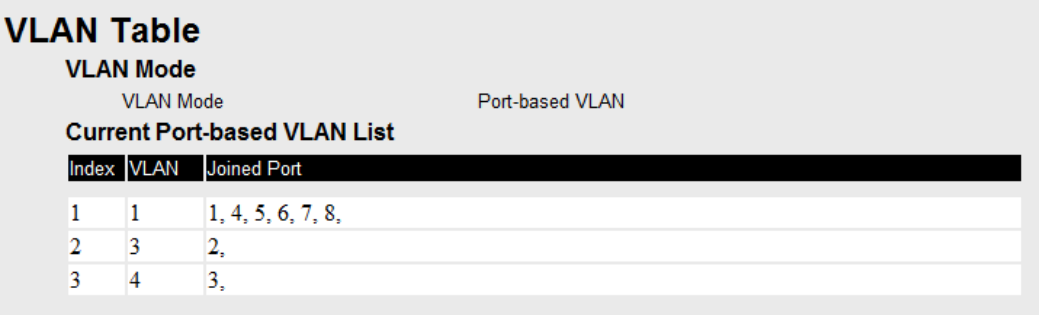
VLAN Mode 802.1Q VLAN

Management VLAN

Management VLAN 1

Current 802.1Q VLAN List

Index	VID	Joined Access Port	Joined Trunk Port	Joined Hybrid Port
1	1	1, 2, 4, 5, 7, 8,	3,	6,



VLAN Table

VLAN Mode

VLAN Mode Port-based VLAN

Current Port-based VLAN List

Index	VLAN	Joined Port
1	1	1, 4, 5, 6, 7, 8,
2	3	2,
3	4	3,

In **802.1Q VLAN table**, you can review the VLAN groups that were created, **Joined Access Ports**, **Trunk Ports** and **Hybrid Ports**. In **Port-based VLAN table**, you can review the VLAN group and joined ports.

NOTE: The Weidmüller managed switches have a maximum of 64 VLAN settings.

3.8 Using Multicast Filtering

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your Weidmüller switch.

3.8.1 The Concept of Multicast Filtering

What is an IP Multicast?

A *multicast* is a packet sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations on a LAN or VLAN that belong to the multicast group. Multicast group members can be distributed across multiple subnets, so that multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only *one* copy of the desired information across the network until the delivery path that reaches group members diverges. To make more efficient use of network bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

The benefits of using IP multicast are:

- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- It works with other IP protocols and services, such as Quality of Service (QoS).

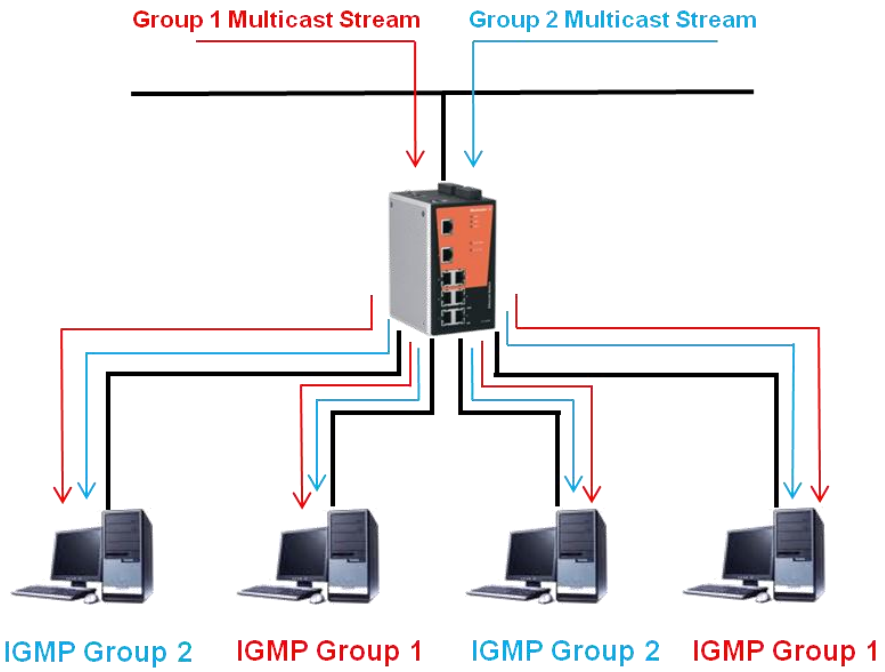
Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all end-stations would cause a substantial reduction in network performance. Furthermore, several industrial automation protocols, such as EtherNet/IP, Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use multicast. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves without multicast filtering, and with multicast filtering.

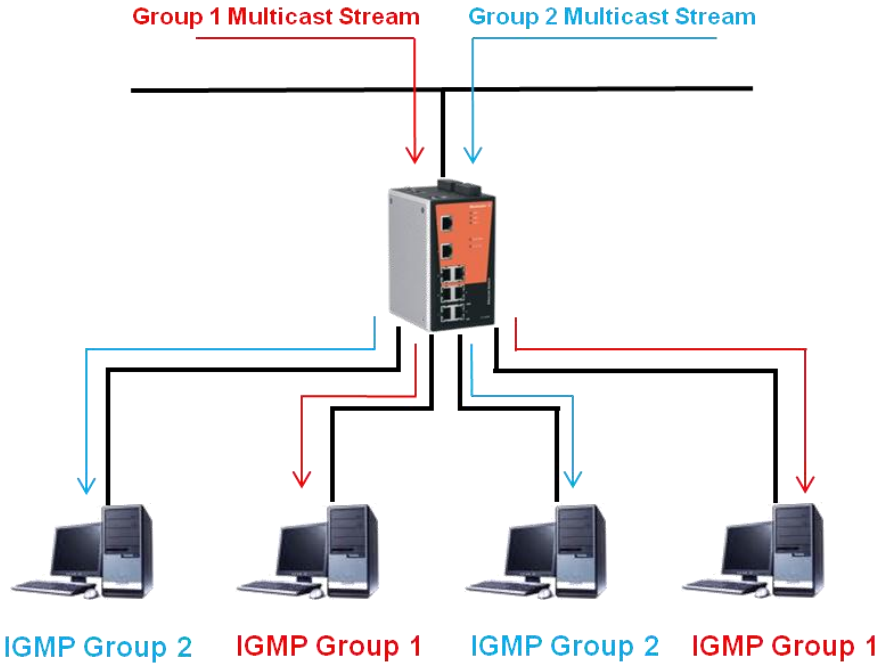
Network without multicast filtering

All hosts receive the multicast traffic, even if they don't need it.



Network with multicast filtering

Hosts only receive dedicated traffic from other hosts belonging to the same group.



The Weidmüller switch has three ways to achieve multicast filtering: IGMP (Internet Group Management Protocol) Snooping, GMRP (GARP Multicast Registration Protocol), and adding a static multicast MAC manually to filter multicast traffic automatically.

IGMP (Internet Group Management Protocol)

Snooping Mode

Snooping Mode allows your switch to forward multicast packets only to the appropriate ports. The switch "snoops" on exchanges between hosts and an IGMP device, such as a router, to find those ports that want to join a multicast group, and then configure its filters accordingly.

IGMP Snooping Enhanced Mode

Snooping Enhanced Mode allows your switch to forward multicast packets to the Weidmüller switch member port only. If you disable Enhanced Mode, data streams will run to the querier port as well as the member port.

Querier Mode

Querier mode allows the Weidmüller switch to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs. IGMP querying is enabled by default on the switch to help prevent interoperability issues with some multicast routers that may not follow the lowest IP address election method. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers).

IGMP querying is enabled by default on the Weidmüller switch to ensure proceeding query election. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers). Query mode allows users to enable IGMP snooping by VLAN ID. Weidmüller switches support IGMP snooping version 1 and version 2. Version 2 is compatible with version 1.The default setting is IGMP V1/V2. "

IGMP Multicast Filtering

IGMP is used by IP-supporting network devices to register hosts with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router, and on other network devices that support multicast filtering. Weidmüller switches support IGMP version 1 and 2. IGMP version 1 and 2 work as follows:

- The IP router (or querier) periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with IP address lower than the IP address of any other IGMP querier connected to the LAN or VLAN can become the IGMP querier.
- When an IP host receives a query packet, it sends a report packet back that identifies the multicast group that the end-station would like to join.
- When the report packet arrives at a port on a switch with IGMP Snooping enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.
- When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
- When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

IGMP version comparison

IGMP Version	Main Features	Reference
V1	Periodic query	RFC-1112
V2	Compatible with V1 and adds: • Group-specific query • Leave group messages • Resends specific queries to verify leave message was the last one in the group • Querier election	RFC-2236

GMRP (GARP Multicast Registration Protocol)

Weidmüller managed switches support IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol), which differs from IGMP (Internet Group Management Protocol). GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or de-register Group membership information dynamically. GMRP functions similarly to GVRP, except that GMRP registers multicast addresses on ports. When a port receives a ***GMRP-join*** message, it will register the multicast address to its database if the multicast address is not registered, and all the multicast packets with that multicast address are able to be forwarded from this port. When a port receives a ***GMRP-leave*** message, it will de-register the multicast address from its database, and all the multicast packets with this multicast address are not able to be forwarded from this port.

Static Multicast MAC

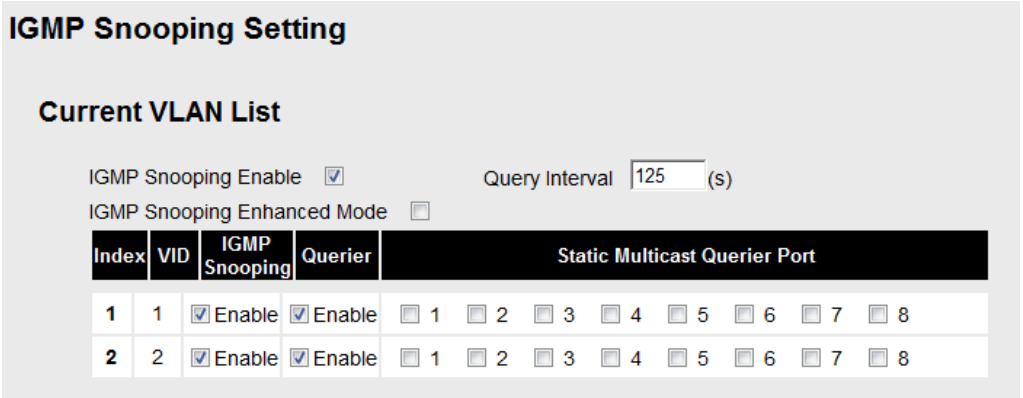
Some devices may only support multicast packets, but not support either IGMP Snooping or GMRP. The Weidmüller switch supports adding multicast groups manually to enable multicast filtering.

Enabling Multicast Filtering

Use the serial console or web interface to enable or disable IGMP Snooping and IGMP querying. If IGMP Snooping is not enabled, then IP multicast traffic is always forwarded, flooding the network.

3.8.2 Configuring IGMP Snooping

IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.


IGMP Snooping Setting
Current VLAN List
IGMP Snooping Enable
Query Interval 125 (s)
IGMP Snooping Enhanced Mode
Index VID IGMP Snooping Querier Static Multicast Querier Port
1 1 Enable Enable 1 2 3 4 5 6 7 8
2 2 Enable Enable 1 2 3 4 5 6 7 8

IGMP Snooping Enable

Setting	Description	Factory Default
Enable/Disable	Checkmark the **IGMP Snooping Enable** checkbox to enable the IGMP Snooping function globally.	Disabled

Query Interval

Setting	Description	Factory Default
Numerical value, input by the user	Sets the query interval of the Querier function globally. Valid settings are from 20 to 600 seconds.	125 seconds

IGMP Snooping Enhanced Mode

Setting	Description	Factory Default
Enable	IGMP Multicast packets will be forwarded to: • Auto-Learned Multicast Querier Ports • Member Ports	Disable
Disable	IGMP Multicast packets will be forwarded to: • Auto-Learned Multicast Router Ports • Static Multicast Querier Ports • Querier Connected Ports • Member Ports	

IGMP Snooping

Setting	Description	Factory Default
Enable/Disable	Enables or disables the IGMP Snooping function on that particular VLAN.	Enabled if IGMP Snooping is enabled globally

NOTE: We suggest the following IGMP Snooping configuration settings:

When the network is mixed with third party switches, such as Cisco:

- "IGMP Snooping Enable" → Enable
- "IGMP Snooping Enhanced Mode" → Disable

When the network consists entirely of Weidmüller switches:

- "IGMP Snooping Enable" → Disable
- "IGMP Snooping Enhanced Mode" → Enable

Querier

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the querier function.	Enabled if IGMP Snooping is enabled globally

Static Multicast Querier Port

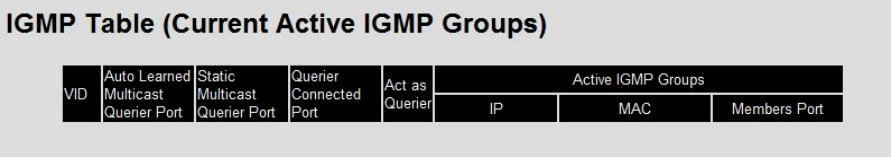
Setting	Description	Factory Default
Select/Deselect	Select the ports that will connect to the multicast routers. These ports will receive all multicast packets from the source. This option is only active when IGMP Snooping is enabled.	Disabled

If a router or layer 3 switch is connected to the network, it will act as the Querier, and consequently this Querier option will be disabled on all Weidmüller layer 2 switches.

If all switches on the network are Weidmüller layer 2 switches, then only one layer 2 switch will act as Querier.

3.8.3 IGMP Table

The IGMP table displays the current active IGMP groups that were detected.

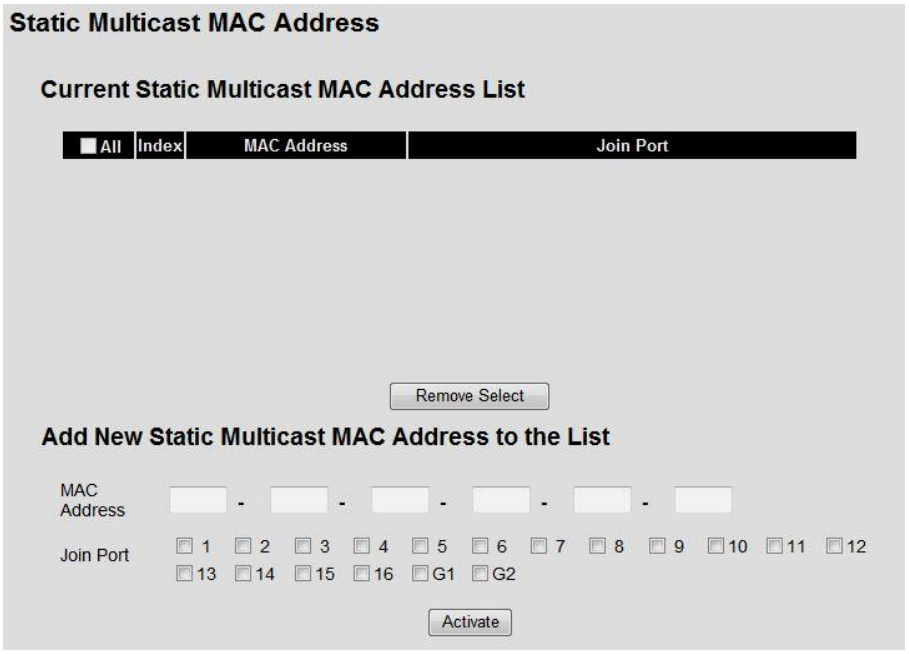


The information shown in the table includes:

- Auto-learned Multicast Router Port: This indicates that a multicast router connects to/sends packets from these port(s)
- Static Multicast Router Port: Displays the static multicast querier port(s)
- Querier Connected Port: Displays the port which is connected to the querier.
- Act as a Querier: Displays whether or not this VLAN is a querier (winner of a election).

3.8.4 Static Multicast MAC Addresses

If required, the Weidmüller switch also supports adding multicast groups manually.



Add New Static Multicast Address to the List

Setting	Description	Factory Default
MAC Address	Input the multicast MAC address of this host.	None

MAC Address

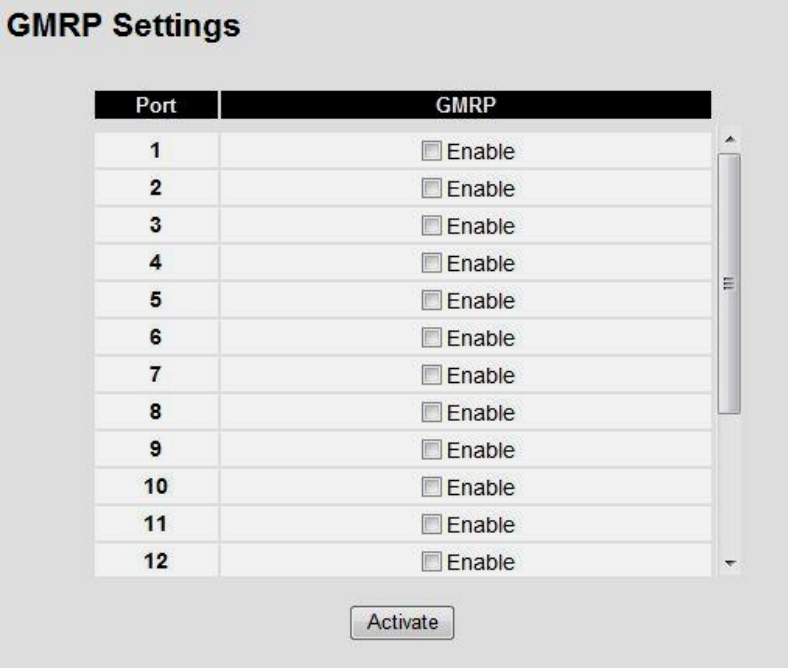
Setting	Description	Factory Default
Integer	Input the number of the VLAN that the host with this MAC address belongs to.	None

Join Port

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to select the join ports for this multicast group.	None

3.8.5 Configuring GMRP

GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or un-register Group membership information dynamically.



GMRP enable

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the GMRP function for the port listed in the Port column	Disable

3.8.6 GMRP Table

The GMRP table displays the current active GMRP groups that were detected.

Setting	Description
Fixed Ports	This multicast address is defined by static multicast.
Learned Ports	This multicast address is learned by GMRP.

3.9 Using Bandwidth Management

In general, one host should not be allowed to occupy unlimited bandwidth, particularly when the device malfunctions. For example, so-called “broadcast storms” could be caused by an incorrectly configured topology, or a malfunctioning device. Weidmüller industrial Ethernet switches not only prevents broadcast storms, but can also be configured to a different ingress rate for all packets, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

3.9.1 Configuring Bandwidth Management

There are two two types of bandwidth management settings available, depending on the specific model of switch.

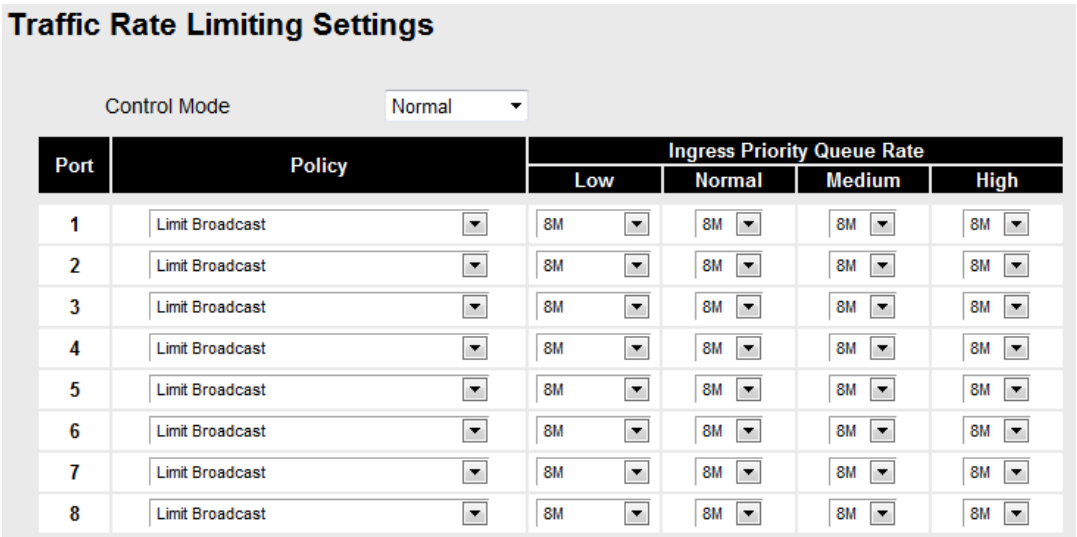
Type	Models Supported
Type 1	IE-SW-VL05M/VL08M series, IE-SW-PL06M/PL08M/PL09M/PL10M series
Type 2	IE-SW-PL16M/PL18M series

Type 1 (IE-SW-VL05M/VL08M series, IE-SW-PL06M/PL08M/PL09M/PL10M series)

Traffic Rate Limiting Settings – Type 1

Control Mode	Description	Factory Default
Normal	Set the max. ingress rate limit for different packet types	Normal
Port Disable	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for a certain period. During this period, all packets from this port will be discarded.	

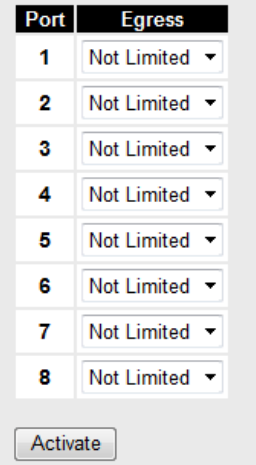
Ingress Rate Limit - Normal – Type 1


Traffic Rate Limiting Settings
Control Mode
Normal
Port
Policy
Ingress Priority Queue Rate
Low
Normal
Medium
High
1 Limit Broadcast 8M 8M 8M 8M
2 Limit Broadcast 8M 8M 8M 8M
3 Limit Broadcast 8M 8M 8M 8M
4 Limit Broadcast 8M 8M 8M 8M
5 Limit Broadcast 8M 8M 8M 8M
6 Limit Broadcast 8M 8M 8M 8M
7 Limit Broadcast 8M 8M 8M 8M
8 Limit Broadcast 8M 8M 8M 8M

Ingress Rate Limit - Normal – Type 1

Policy	Description	Factory Default
Limit All	Select the ingress rate limit for different packet types from the following options: Not Limited, 128K, 256K, 512K, 1M, 2M, 4M, 8M	Limit Broadcast 8M
Limit Broadcast, Multicast, Flooded Unicast		
Limit Broadcast, Multicast		
Limit Broadcast		

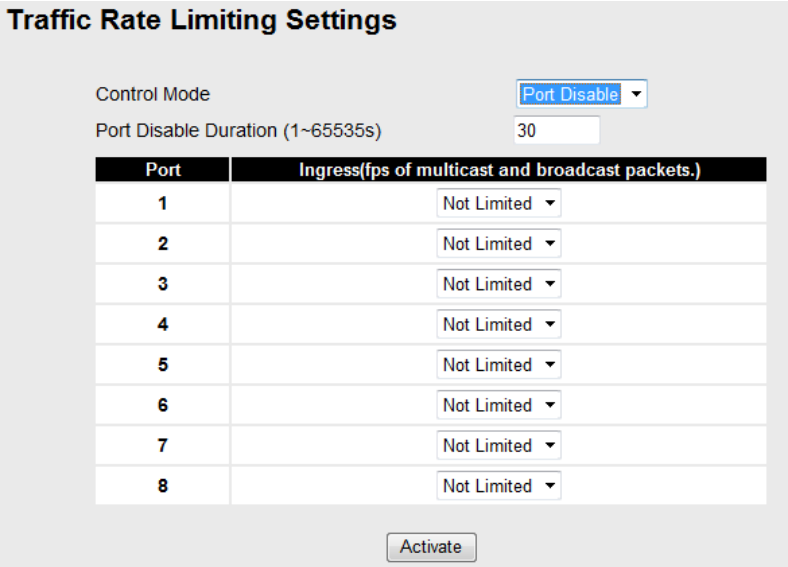
Egress Rate Limit –Normal – Type 1



Egress Rate Limit –Normal – Type 1

Setting	Description	Factory Default
Egress rate	Select the egress rate limit (% of max. throughput) for all packets from the following options: Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Not Limited

Ingress Rate Limit – Port Disable



Ingress Rate Limit – Port Disable

Setting	Description	Factory Default
Port disable duration (1~65535 seconds)	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for this period of time. During this time, all packets from this port will be discarded.	30 second
Ingress (fps)	Select the ingress rate (fps) limit for all packets from the following options: Not Limited, 4464, 7441, 14881, 22322, 37203, 52084, 74405	Not Limited

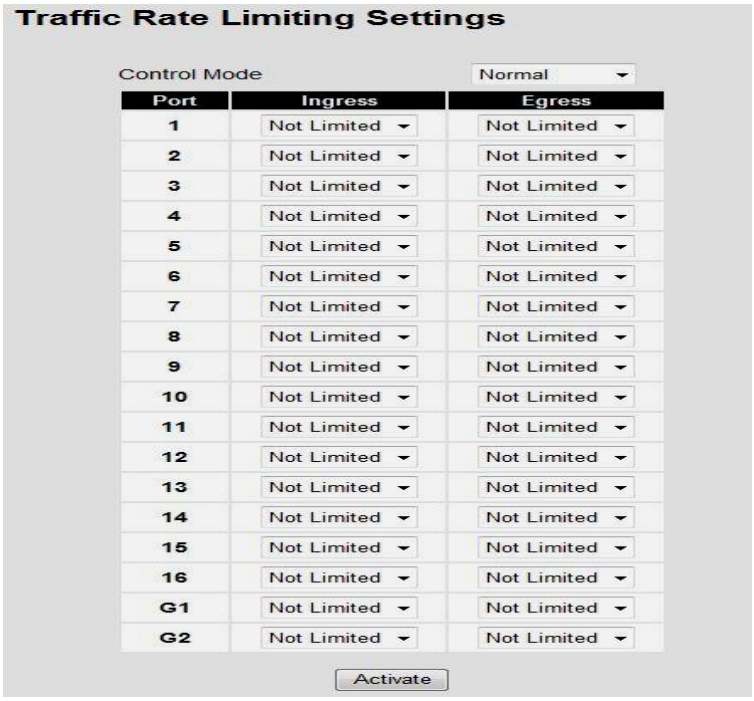
Type 2 (IE-SW-PL16M/PL18M series)

Broadcast Storm Protection – Type 2

Enable/Disable – Type 2

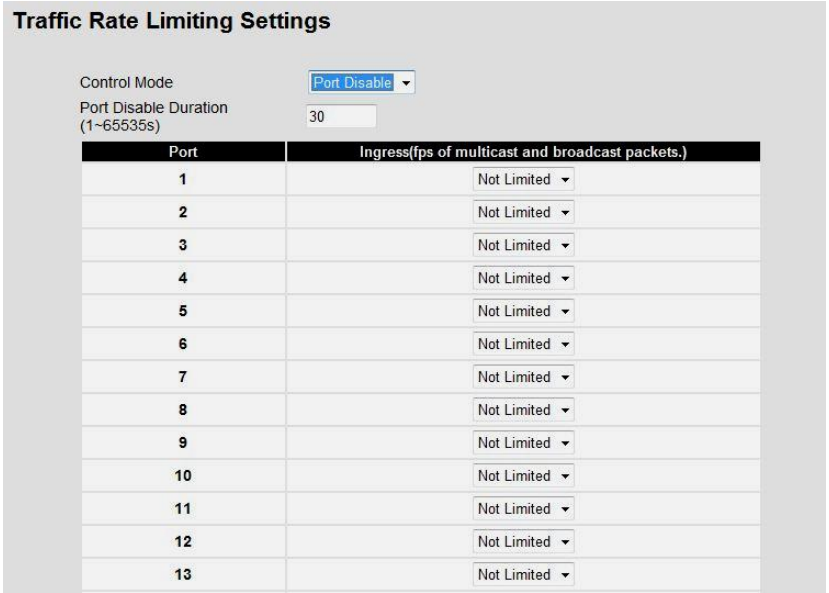
Setting	Description	Factory Default
Enable/Disable	Enables or disables Broadcast Storm Protection for unknown broadcast packet globally	Enable
	Enables or disables Broadcast Storm Protection for unknown multicast packets globally	Disable

3.9.2 Traffic Rate Limiting Settings


Traffic Rate Limiting Settings
Control Mode
Normal
Port
Ingress
Egress
1 Not Limited Not Limited
2 Not Limited Not Limited
3 Not Limited Not Limited
4 Not Limited Not Limited
5 Not Limited Not Limited
6 Not Limited Not Limited
7 Not Limited Not Limited
8 Not Limited Not Limited
9 Not Limited Not Limited
10 Not Limited Not Limited
11 Not Limited Not Limited
12 Not Limited Not Limited
13 Not Limited Not Limited
14 Not Limited Not Limited
15 Not Limited Not Limited
16 Not Limited Not Limited
G1 Not Limited Not Limited
G2 Not Limited Not Limited
Activate

Ingress and Egress Rate Limit - Normal

Setting	Description	Factory Default
Ingress rate	Select the ingress/egress rate limit (% of max throughput) for all packets from the following options:Nnot limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	N/A
Egress rate		



Ingress Rate Limit – Port Disable

Setting	Description	Factory Default
Period (1 ~ 65535 seconds)	When the ingress packets exceed the ingress rate limit, the port will be disabled for a certain period.	30 seconds
Ingress (frame per second)	Select the ingress rate (fps) limit for all packets from the following options: Not limited, 4464, 7441, 14881, 22322, 37202, 52084, 74405	Not limited

3.10 Using Auto Warning

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet switch that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The Weidmüller switch supports different approaches to warn engineers automatically, such as email and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

3.10.1 Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place. Three basic steps are required to set up the Auto Warning function:

Configure Email Event Types

Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Email Alarm Events setting* subsection).

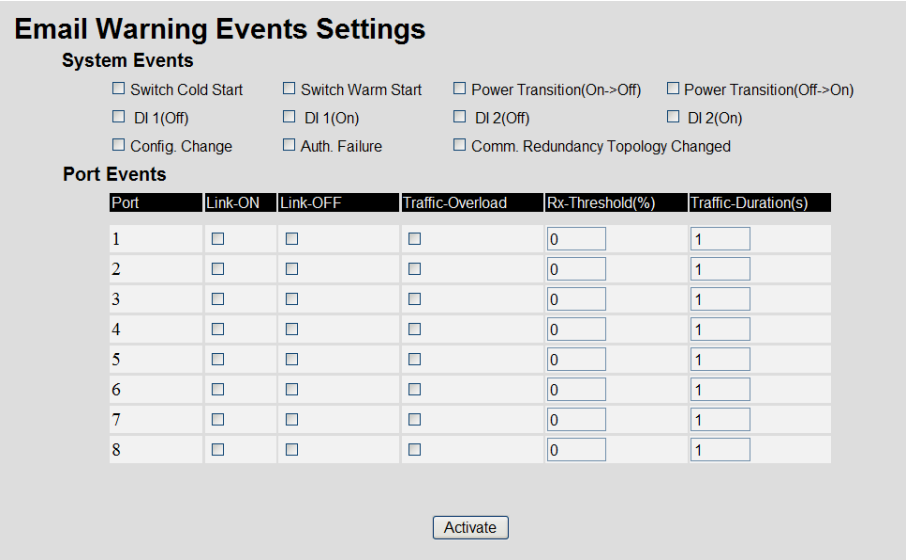
Configure Email Settings

To configure a Weidmüller switch's email setup from the serial, Telnet, or web console, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address to which warning messages will be sent.

Activate your settings and if necessary, test the email

After configuring and activating your Weidmüller switch's Event Types and Email Setup, you can use the **Test Email** function to see if your e-mail addresses and mail server address have been properly configured.

3.10.2 Event Types



Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

System Events	Warning e-mail is sent when…
Switch Cold Start	Power is cut off and then reconnected.
Switch Warm Start	Weidmüller switch is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	Weidmüller switch is powered down.
Power Transition (Off→On)	Weidmüller switch is powered up.
DI1 (On→Off)	Digital Input 1 is triggered by on to off transition
DI1 (Off→On)	Digital Input 1 is triggered by off to on transition
DI2 (On→Off)	Digital Input 2 is triggered by on to off transition
DI2 (Off→On)	Digital Input 2 is triggered by off to on transition
Configuration Change Activated	Any configuration item has been changed.
Authentication Failure	An incorrect password was entered.
Comm. Redundancy Topology Changed	If any Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). If the Master of the Turbo Ring has changed or the backup path is activated.

Port Events	Warning e-mail is sent when…
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).

Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%) (0 to 100 %)	Enter a non-zero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.) (1 to 300 sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.

NOTE: The Traffic-Overload, Traffic-Threshold (%) and Traffic-Duration (sec) Port Event items are related. If the Traffic-Overload event is enabled, then ensure to set a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

NOTE: If a warning mail is sent by the Switch the sender mail address automatically is created by combination of the parameters "Switch Name", "Location" (Menu Basic settings → System) and character "@".

Format of sender mail address: < Switch Name>@< Switch Location>.

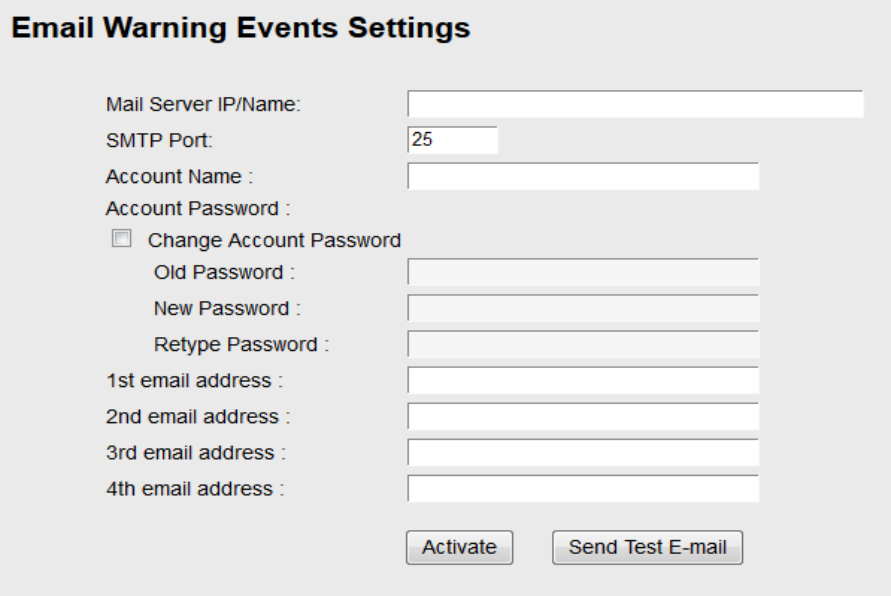
If mail warnings will be used please ensure that the combination of parameters "Switch Name" and "Location" results to be a valid mail address. For this reason the parameter "Switch Name" must be a vaild mail prefix and the parameter "Location" has to be configured like to be a domain name.

Example: Switch Name = **Managed_Switch** and Location = **myDepartment.de**

Automatically created sender mail address = **Managed_Switch@myDepartment.de**

► Do **not** use blanks or special characters for both parameters which would result in an unvalid mail address otherwise the receiving mail server would not accept the warning mail.

3.10.3 Email Settings



Mail Server IP/Name

Setting	Description	Factory Default
IP address or name	The IP Address or name of your email server.	None

SMTP Port

Setting	Description	Factory Default
SMTP port	Display the SMTP port number	25

Account Name

Setting	Description	Factory Default
Max. 45 characters	Your email account	None

Password Setting

Setting	Description	Factory Default
Disable/Enable to change password	To reset the password from the Web Browser interface, click the Change password check-box, type the Old password, type the New password, retype the New password, and then click Activate (Max. of 45 characters).	Disable
Old password	Type the current password when changing the password	None
New password	Type new password when enabled to change password; Max. 45 characters.	None
Retype password	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	None

Email Address

Setting	Description	Factory Default
Max. of 30 characters	You can set up to 4 email addresses to receive alarm emails from the Weidmüller switch.	None

Send Test Email

After you complete the email settings, you should first click **Activate** to activate those settings, and then press the **Send Test Email** button to verify that the settings are correct.

NOTE: Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism.

We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.

3.10.4 Configuring Relay Warnings

The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

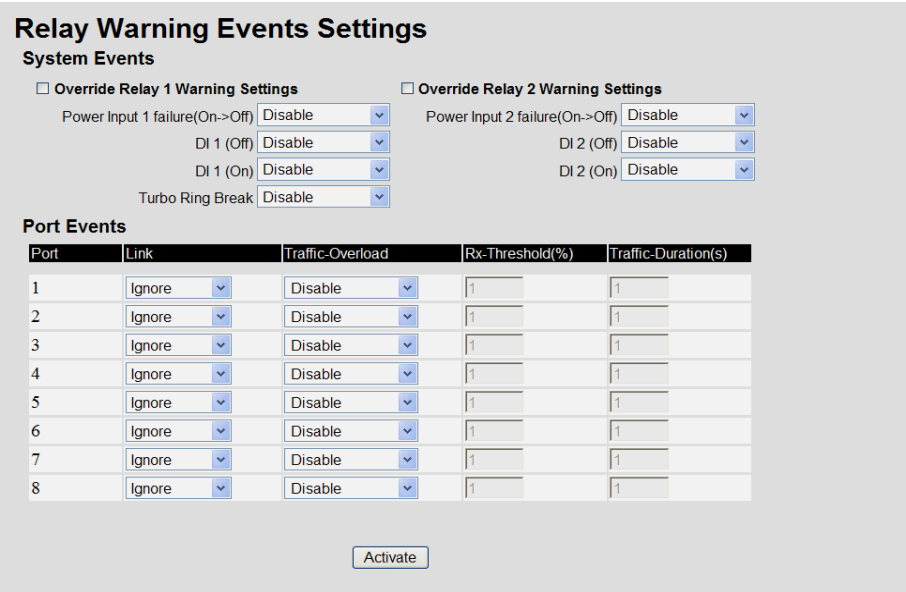
Configure Relay Event Types

Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Relay Warning Events Settings* subsection).

Activate your settings

After completing the configuration procedure you will need to activate your Weidmüller switch's Relay Event Types.

Configuring Relay Warning Events Settings


Relay Warning Events Settings
System Events
Override Relay 1 Warning Settings
Power Input 1 failure(On->Off) Disable
DI 1 (Off) Disable
DI 1 (On) Disable
Turbo Ring Break Disable
Override Relay 2 Warning Settings
Power Input 2 failure(On->Off) Disable
DI 2 (Off) Disable
DI 2 (On) Disable
Port Events
Port Link Traffic-Overload Rx-Threshold(%) Traffic-Duration(s)
1 Ignore Disable 1 1
2 Ignore Disable 1 1
3 Ignore Disable 1 1
4 Ignore Disable 1 1
5 Ignore Disable 1 1
6 Ignore Disable 1 1
7 Ignore Disable 1 1
8 Ignore Disable 1 1
Activate

Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

The Weidmüller switch supports two relay outputs. You can configure which relay output is related to which events, which helps administrators identify the importance of the different events.

System Events	Warning Relay output is triggered when…
Power Transition (On -> Off)	Weidmüller switch is powered down
Power Transition (Off -> On)	Weidmüller switch is powered up
DI1 (On→Off)	Digital Input 1 is triggered by on to off transition
DI1 (Off→On)	Digital Input 1 is triggered by off to on transition
DI2 (On→Off)	Digital Input 2 is triggered by on to off transition
DI2 (Off→On)	Digital Input 2 is triggered by off to on transition
Turbo Ring Break	The Turbo Ring is broken. Only the MASTER switch of Turbo Ring will output warning relay.

Port Events	Warning e-mail is sent when…
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%) (0 to 100 %)	Enter a nonzero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.) (1 to 300 sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.

NOTE: The Traffic-Overload, Traffic-Threshold (%), and Traffic-Duration (sec) Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a non-zero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

Override relay alarm settings

Select this option to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition.

Warning List

The Current Warning List can be used to see if any relay alarms have been issued.

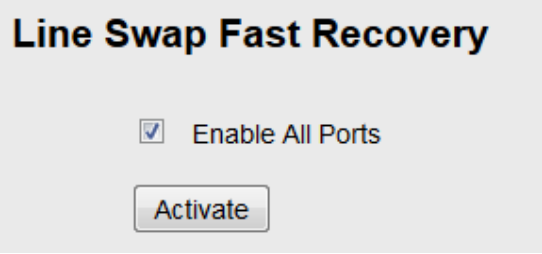
Current Warning List

Index	Event	Relay
1	Power Input 2 On->Off !	1
2	DI 1 Off !	1
3	DI 2 Off !	2
4	Port 3 Link Off !	1

3.11 Line-Swap-Fast-Recovery

The Line-Swap Fast Recovery function, which is enabled by default, allows the Weidmüller switch to return to normal operation extremely quickly after devices are unplugged and then re-plugged into different ports. The recovery time is on the order of a few milliseconds (compare this with standard commercial switches for which the recovery time could be on the order of several minutes). To disable the Line-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access either the Console utility's **Line-Swap recovery** page, or the Web Browser interface's **Line-Swap fast recovery** page, as shown below.

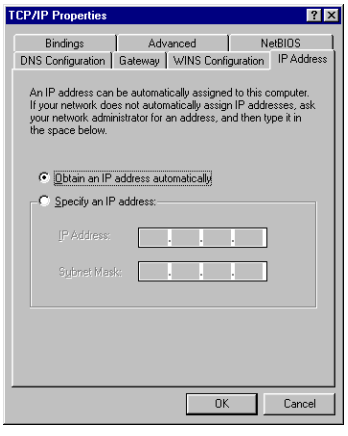
3.11.1 Configuring Line-Swap Fast Recovery



Enable Line-Swap-Fast-Recovery

Setting	Description	Factory Default
Enable/Disable	Checkmark the checkbox to enable the Line-Swap-Fast-Recovery function	Enable

3.12 Set Device IP


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

To reduce the effort required to set up IP addresses, the Weidmüller switch comes equipped with DHCP/BootP server and RARP protocol to set up IP addresses of Ethernet-enabled devices automatically.

When enabled, the **Set device IP** function allows the Weidmüller switch to assign specific IP addresses automatically to connected devices that are equipped with *DHCP Client* or *RARP* protocol. In effect, the Weidmüller switch acts as a DHCP server by assigning a connected device with a specific IP address stored in its internal memory. Each time the connected device is switched on or rebooted, the Weidmüller switch sends the device

the desired IP address.

Take the following steps to use the **Set device IP** function:

STEP 1 → **S**et up the connected devices

Set up those Ethernet-enabled devices connected to the Weidmüller switch for which you would like IP addresses to be assigned automatically. The devices must be configured to obtain their IP address automatically.

The devices' configuration utility should include a setup page that allows you to choose an option similar to the *Obtain an IP address automatically* option.

For example, Windows' TCP/IP Properties window is shown at the right. Although your device's configuration utility may look quite a bit different, this figure should give you some idea of what to look for.

You also need to decide which of the Weidmüller switch's ports your Ethernet-enabled devices will be connected to. You will need to set up each of these ports separately, as described in the following step

STEP 2

Configure the Weidmüller switch's **Set device IP** function, either from the Console interface or from the Web Browser interface. In either case, you simply need to enter the **Desired IP** for each port that needs to be configured.

STEP 3

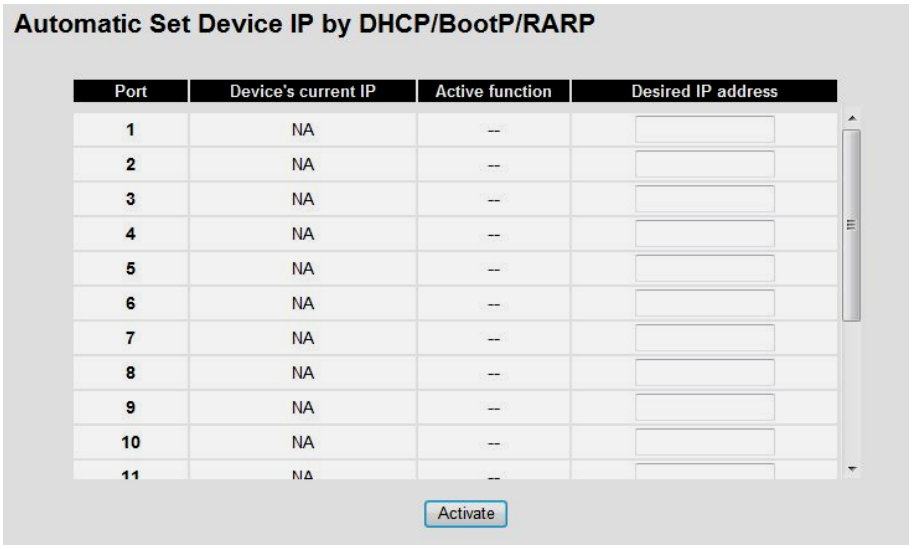
Be sure to activate your settings before exiting.

When using the Web Browser interface, activate by clicking on the Activate button.

When using the Console interface, activate by first highlighting the **Activate** menu option, and then press **Enter**. You should receive the **Set device IP settings are now active! (Press any key to continue)** message.

3.12.1 Configuring Set Device IP

Automatic "Set Device IP" by DHCP/BootP/RARP



Desired IP Address

Setting	Description	Factory Default
IP Address	Set the desired IP of connected devices.	None

3.12.2 DHCP Relay Agent (Option 82)

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

DHCP Option 82 is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

When Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains 2 sub-options: Circuit ID and Remote ID, which define the relationship between end device IP and the DHCP Option 82 server. The **Circuit ID** is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID. The format of the **Circuit ID** is as described below:

FF–VV–VV–PP

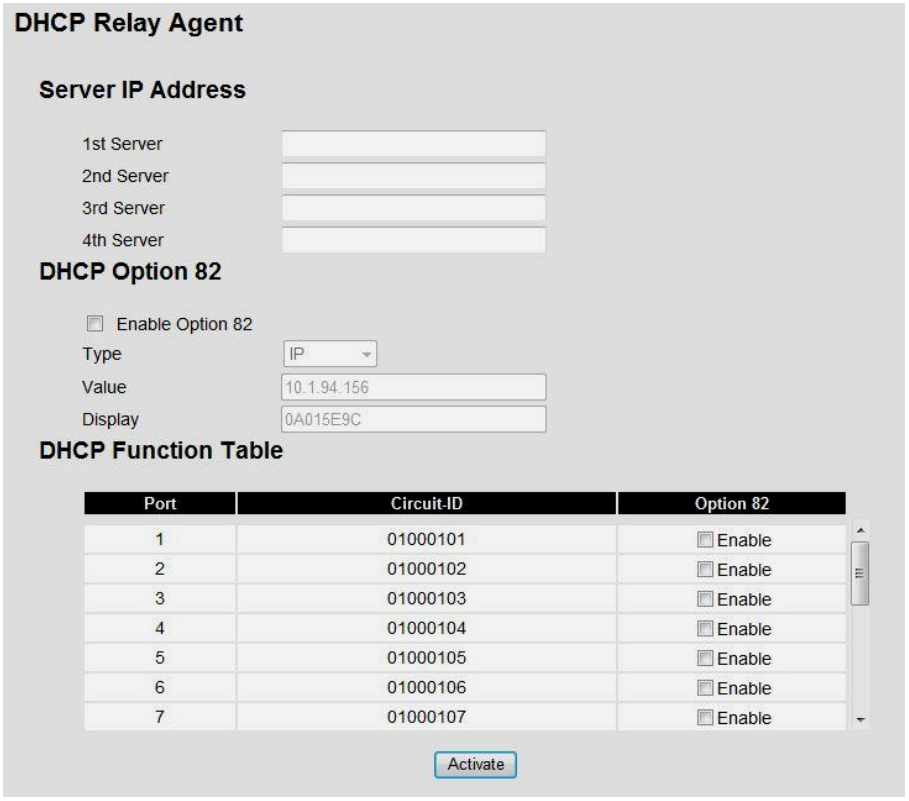
Where the first byte "FF" is fixed to "01", the second and the third byte "VV-VV" is formed by the port VLAN ID in hex, and the last byte "PP" is formed by the port number in hex. For example,

01–00–0F–03 is the "Circuit ID" of port number 3 with port VLAN ID 15.

The "Remote ID" is to identify the relay agent itself and it can be one of the following:

- The IP address of the relay agent.
- The MAC address of the relay agent.
- A combination of IP address and MAC address of the relay agent.
- A user-defined string.

Configuring DHCP Relay Agent



Server IP Address

1st Server

Setting	Description	Factory Default
IP address for the 1st DHCP server	Assigns the IP address of the 1st DHCP server that the switch tries to access.	None

2nd Server

Setting	Description	Factory Default
IP address for the 2nd DHCP server	Assigns the IP address of the 2nd DHCP server that the switch tries to access.	None

3rd Server

Setting	Description	Factory Default
IP address for the 3rd DHCP server	Assigns the IP address of the 3rd DHCP server that the switch tries to access.	None

4th Server

Setting	Description	Factory Default
IP address for the 4th DHCP server	Assigns the IP address of the 4th DHCP server that the switch tries to access.	None

DHCP Option 82

Enable Option 82

Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function.	Disable

Type

Setting	Description	Factory Default
IP	Uses the switch's IP address as the remote ID sub.	IP
MAC	Uses the switch's MAC address as the remote ID sub.	IP
Client-ID	Uses a combination of the switch's MAC address and IP address as the remote ID sub.	IP
Other	Uses the user-designated ID sub.	IP

Value

Setting	Description	Factory Default
Max. 12 characters	Displays the value that was set. Complete this field if type is set to Other.	Switch IP address

Display

Setting	Description	Factory Default
read-only	The actual hexadecimal value configured in the DHCP server for the Remote-ID. This value is automatically generated according to the Value field. Users cannot modify it.	COA87FFD

DHCP Function Table

Option 82

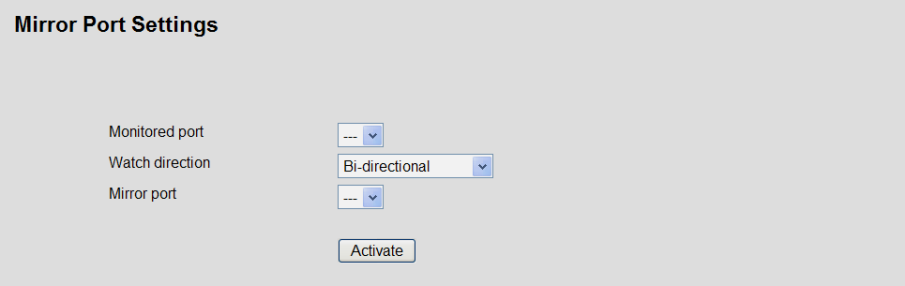
Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function for this port.	Disable

3.13 Using Diagnosis

The Weidmüller switch provides three important tools for administrators to diagnose network systems.

3.13.1 Mirror Port

The **Mirror port** function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the *mirror port*) to receive the same data being transmitted from, or both to and from, the port under observation. This allows the network administrator to **sniff** the observed port and thus keep tabs on network activity.



Perform the following steps to set up the **Mirror Port** function:

STEP 1

Configure the **Mirror Port** function from either the Console interface or Web Browser interface. You will need to configure three settings:

Mirror Port Settings

Setting	Description
Monitored Port	Select one port whose network activity will be monitored.
Watch Direction	Select one of the following three watch direction options: • **Input data stream** Select this option to monitor only those data packets coming in through the monitored port. • **Output data stream** Select this option to monitor only those data packets being sent out through the monitored port. **Bi-directional** Select this option to monitor data packets both coming into, and being sent out through, the monitored port.
Mirror Port	Select one port that will be used to monitor the activity of the monitored port.

STEP 2

Be sure to activate your settings before exiting.

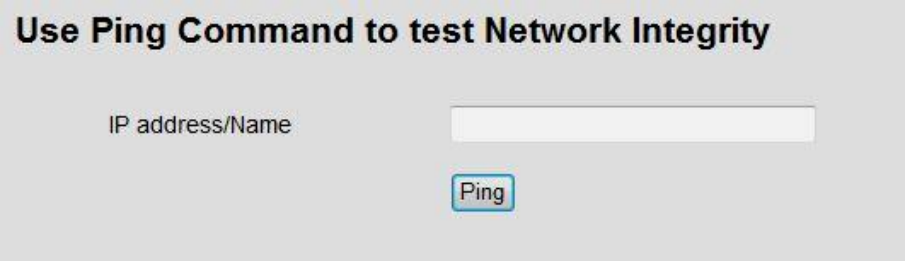
- When using the Web Browser interface, activate by clicking **Activate**.

- When using the Console interface, activate by first highlighting the Activate menu option, and then press **Enter**. You should receive the **Mirror port settings are now active! (Press any key to continue)** message.

3.13.2 Ping

The **Ping** function uses the *ping* command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the Weidmüller switch itself. In this way, the user can essentially sit on top of the Weidmüller switch and send ping commands out through its ports.

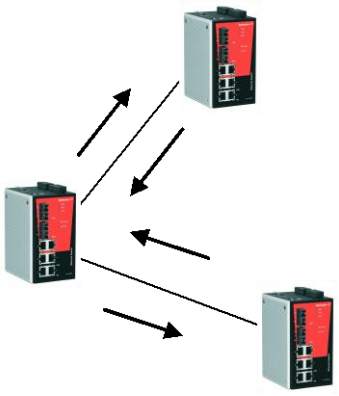
To use the Ping function, type in the desired IP address, and then press **Enter** from the Console utility, or click **Ping** when using the Web Browser interface.



3.13.3 LLDP Function

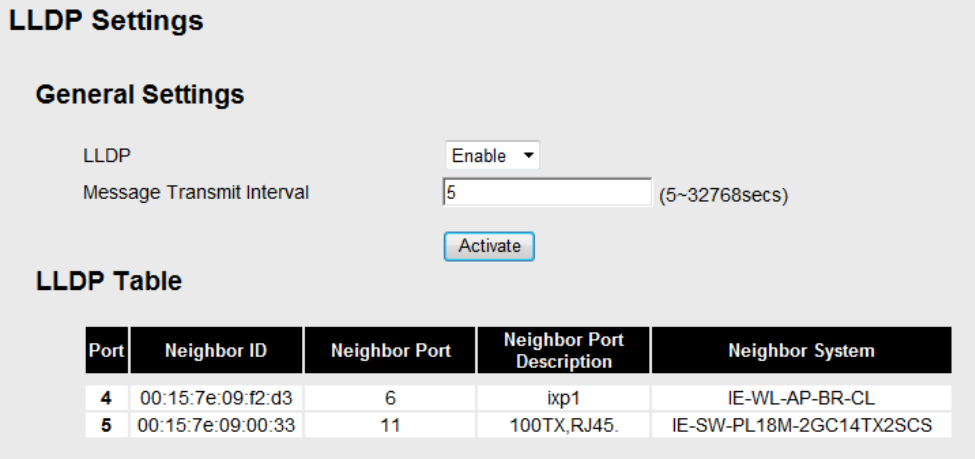
3.13.3.1 Overview

Defined by IEEE 802.11AB, LLDP is an OSI Layer 2 Protocol that standardizes the methodology of self-identity advertisement. It allows each networking device, e.g. a Weidmüller managed switch, to periodically inform its neighbors about its self-information and configurations. As a result, all of the devices would have knowledge about each other; and through SNMP, this knowledge can be transferred to a Network Management Software for auto-topology and network visualization.



From the switch's web interface, users have the option of either enabling or disabling the LLDP, as well as setting the LLDP transmit interval (as shown in the figure below). In addition, users are able to view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows a Network Management Software to automatically display the network's topology as well as system setup details such as VLAN, and Trunking for the entire network.

3.13.3.2 Configuring LLDP Settings



General Settings

LLDP

Setting	Description	Factory Default
Enable or Disable	Enables or disables the LLDP function.	Enable

Message Transmit Interval

Setting	Description	Factory Default
Numbers from 5 to 32768 sec.	To set the transmit interval of LLDP messages. Unit is in seconds.	5 (seconds)

LLDP Table

The LLDP Table displays the following information:

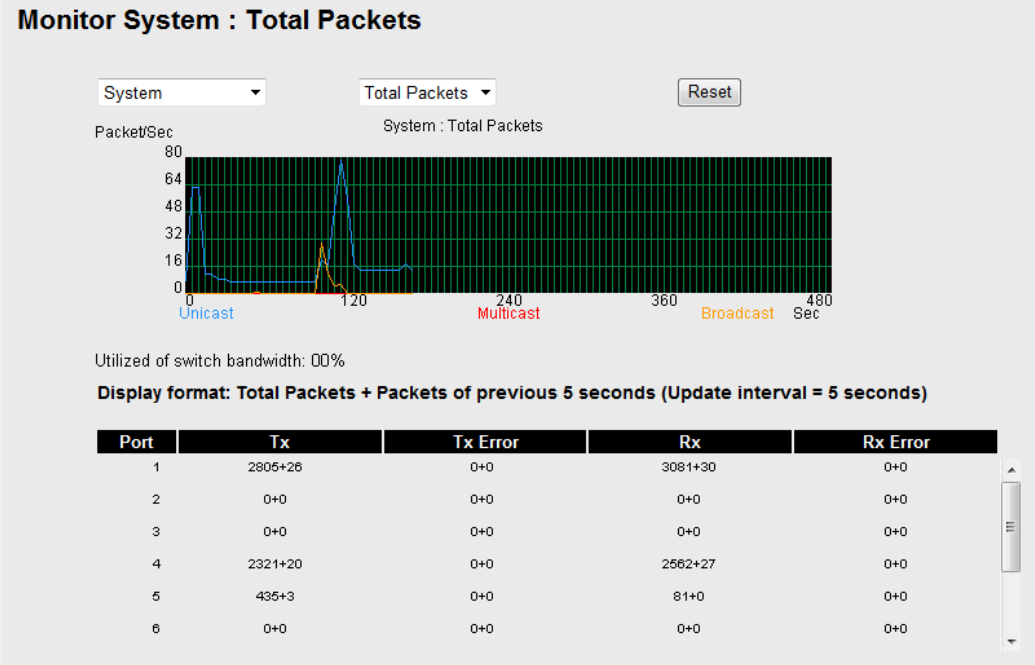
Port	The port number that connects to the neighbor device.
Neighbor ID	A unique entity (typically the MAC address) that identifies a neighbor device.
Neighbor Port	The port number of the neighbor device.
Neighbor Port Description	A textual description of the neighbor device's interface.
Neighbor System	Hostname of the neighbor device.

3.14 Using Monitor

You can monitor statistics in real time from the Weidmüller switch's web console and serial console.

3.14.1 Monitor by Switch

Access the Monitor by selecting "System" from the left selection bar. Monitor by System allows the user to view a graph that shows the combined data transmission activity of all of the switch's ports. Click one of the four options—**Total Packets**, **TX Packets**, **RX Packets**, or **Error Packets**—to view transmission activity of specific types of packets. TX Packets are packets sent out from the Weidmüller switch, RX Packets are packets received from connected devices, and Error Packets are packets that did not pass TCP/IP's error checking algorithm. The Total Packets option displays a graph that combines TX, RX, and TX Error, RX Error Packets activity. The graph displays data transmission activity by showing **Packets/s** (i.e., packets per second, or pps) versus **sec.** (seconds). In fact, three curves are displayed on the same graph: **Unicast** packets (in blue color), **Multicast** packets (in red color), and **Broadcast** packets (in orange color). The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.

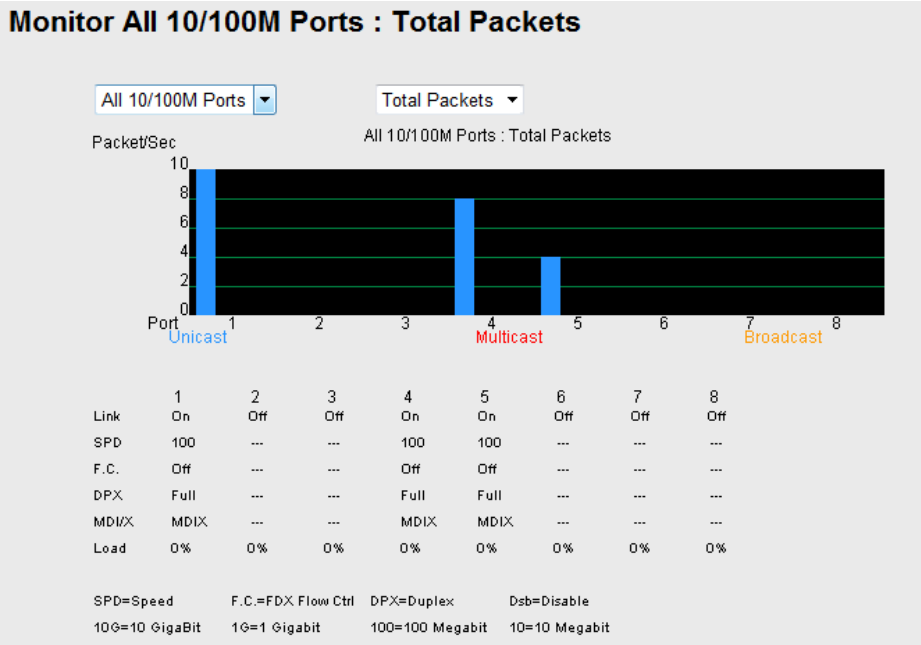


Port	Tx	Tx Error	Rx	Rx Error
1	2805+26	0+0	3081+30	0+0
2	0+0	0+0	0+0	0+0
3	0+0	0+0	0+0	0+0
4	2321+20	0+0	2562+27	0+0
5	435+3	0+0	81+0	0+0
6	0+0	0+0	0+0	0+0

3.14.2 Monitor by Port

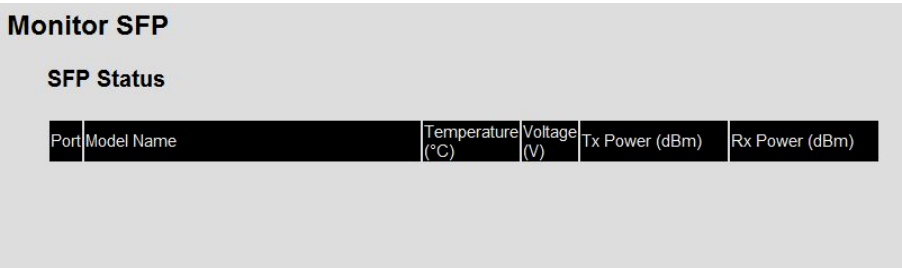
Access the Monitor by Port function by selecting **ALL 10/100M or 1G Ports, or Port *i***, in which ***i*= 1, 2, …, G2** from the left pull-down list. The **Port *i*** options are identical to the Monitor by System function discussed above, in that users can view graphs that show All Packets, TX Packets, RX Packets, or Error Packets activity, but in this case, only for an individual port. The **All Ports** option is essentially a graphical display of the individual port activity that can be viewed with the Console Monitor function discussed above. The All Ports option shows three vertical bars for each port. The height of the bar represents **Packets/s** for the type of packet, at the instant the bar is being viewed. That is, as time progresses, the height of the bar moves up or down so that the user can view the change in the rate of packet transmission. The blue colored bar shows **Unicast** packets, the red colored bar shows **Multicast** packets, and the orange colored bar shows **Broadcast** packets. The

graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



3.14.3 Monitor by SFP

Optical fiber is commonly used for long distance data transmission. However, when link issues occur, it is very costly to trouble shoot the fiber cable and fiber transceiver at remote sites. To solve this problem, Weidmüller industrial Ethernet switches provide digital diagnostic and monitoring functions on Weidmüller SFP optical fiber links and allow users to measure optical parameters and its performance from center site. This function can greatly facilitate the trouble shooting process for optical fiber links and reduce costs for onsite debug.



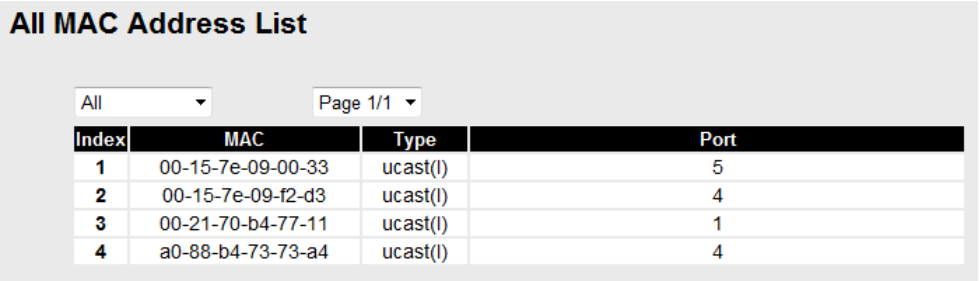
Parameter	Description
Port No.	Switch port number with SFP plugged in
Model Name	Weidmüller SFP model name
Temperature (°C)	SFP casing temperature
Voltage (V)	Voltage supply to the SFP
Tx power (dBm)	The amount of light being transmitted into the fiber optic cable
Rx power (dBm)	The amount of light being received from the fiber optic cable

NOTE: Certain tolerances exist between real data and measured data.

Parameters	Tolerance
Temperature (°C)	± 3°C
Voltage (V)	± 0.1V
Tx power (dBm)	± 3dB
Rx power (dBm)	± 3dB

3.15 Using the MAC Address Table

This section explains the information provided by the Weidmüller switch's MAC address table.



The MAC Address table can be configured to display the following Weidmüller switch MAC address groups, which are selected from the drop-down list:

ALL	Select this item to show all of the Weidmüller switch's MAC addresses.
ALL Learned	Select this item to show all of the Weidmüller switch's Learned MAC addresses.
ALL Static Lock	Select this item to show all of the Weidmüller switch's Static Lock MAC addresses (not supported by Value Line managed Switches).
ALL Static	Select this item to show all of the Weidmüller switch's Static, Static Lock, and Static Multicast MAC addresses.
ALL Static Multicast	Select this item to show all of the Weidmüller switch's Static Multicast MAC addresses.
Port n	Select this item to show all of the MAC addresses dedicated ports.

The table displays the following information:

MAC	This field shows the MAC address.
Type	This field shows the type of this MAC address.

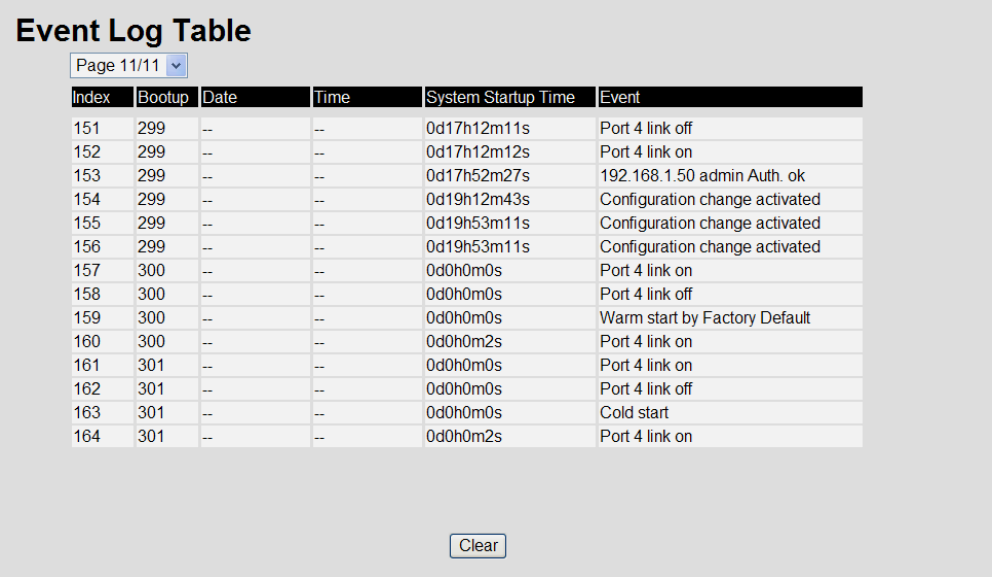
Port	This field shows the port that this MAC address belongs to.

3.16 System Log

The following events will be recorded into the Switch's Event Log table:

- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off → On), Power 1/2 transition (On → Off)
- Authentication fail
- Topology changed
- Master setting is mismatched
- Port traffic overload
- dot1x Auth Fail
- Port link off/on

3.16.1 Using Event Log

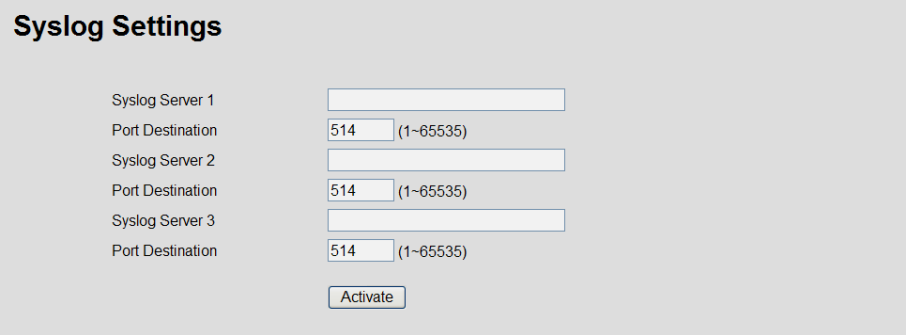

Event Log Table
Page 11/11
Index Bootup Date Time System Startup Time Event
151 299 -- -- 0d17h12m11s Port 4 link off
152 299 -- -- 0d17h12m12s Port 4 link on
153 299 -- -- 0d17h52m27s 192.168.1.50 admin Auth. ok
154 299 -- -- 0d19h12m43s Configuration change activated
155 299 -- -- 0d19h53m11s Configuration change activated
156 299 -- -- 0d19h53m11s Configuration change activated
157 300 -- -- 0d0h0m0s Port 4 link on
158 300 -- -- 0d0h0m0s Port 4 link off
159 300 -- -- 0d0h0m0s Warm start by Factory Default
160 300 -- -- 0d0h0m2s Port 4 link on
161 301 -- -- 0d0h0m0s Port 4 link on
162 301 -- -- 0d0h0m0s Port 4 link off
163 301 -- -- 0d0h0m0s Cold start
164 301 -- -- 0d0h0m2s Port 4 link on
Clear

The Event Log Table displays the following information:

Bootup	This field shows how many times the Weidmüller switch has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the Basic Setting page.
Time	The time is updated based on how the current time is set in the Basic Setting page.
System Startup Time	The system startup time related to this event.
Events	Events that have occurred.

3.16.2 Syslog Settings

This function provides the event logs for the syslog server. The function supports 3 configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a syslog UDP packet to the specified syslog servers. The log data which will be sent to a syslog server is the same as created for the internal Event Log.



Syslog Server 1/2/3

Setting	Description	Factory Default
IP Address	Enter the IP address of Syslog Server 1/2/3 used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of Syslog Server 1/2/3.	514

4. Using Industrial Protocols

4.1 MODBUS/TCP MAP

Introduction

MODBUS TCP is a protocol commonly used for the integration of a SCADA system. It is also a vendor-neutral communication protocol used to monitor and control industrial automation equipment such as PLCs, sensors, and meters. In order to be fully integrated into industrial systems, Weidmüller's switches support Modbus TCP/IP protocol for real-time monitoring in a SCADA system.

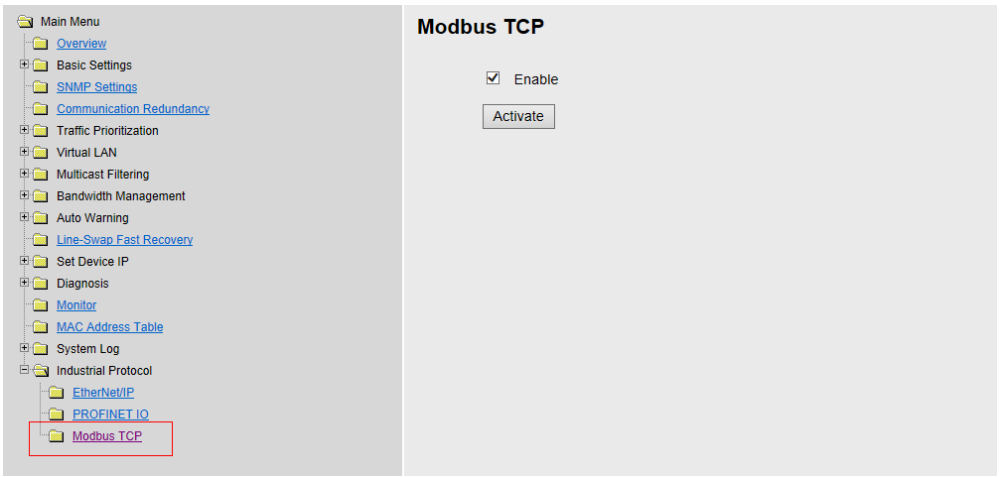
Data Format and Function Code

MODBUS TCP supports different types of data format for reading. The primary four types of them are:

Data Access Type		Function Code	Function Name	Note
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs	
	Internal Bits or Physical Coils	1	Read Coils	
Word access (16-bit access)	Physical Input Registers	4	Read Input Registers	Supported by Weidmüller managed Switches
	Physical Output Registers	3	Read Holding Registers	

Weidmüller switches support **Function Code 4** with **16-bit (2-word)** data access for **read-only** information and using **Unit ID 1.**

Configuring MODBUS/TCP on Weidmüller Switches



Note: Modbus TCP is enabled by default. To disable Modbus TCP, uncheck **Enable Modbus TCP** then click apply.

MODBUS Data Map and Information Interpretation of Weidmüller Switches

The data map addresses of Weidmüller switches shown in the following table start from **MODBUS address 30001** for Function Code 4. For example, the address offset 0x0000 (hex) equals MODBUS address 30001, and the address offset 0x0010 (hex) equals MODBUS address 30017. Note that all the information read from Weidmüller switches are in hex mode. To interpret the information, refer to the ASCII table for the translation (e.g. 0x4D = 'M', 0x6F = 'o').

Address Offset	Data Type	Interpretation	Description
System Information			
0x0000	1 word	HEX	Constant value = 0xFFFF
0x0001	1 word		Unit ID (Ethernet = 1)
0x0002	1 word	HEX	Product Code = 0x0003
0x0010	20 words	ASCII	Vendor Name = "Weidmueller" Word 0 Hi byte = 'W' Word 0 Lo byte = 'e' Word 1 Hi byte = 'i' Word 1 Lo byte = 'd' Word 2 Hi byte = 'm' Word 2 Lo byte = 'u' Word 3 Hi byte = 'e' Word 3 Lo byte = 'l' Word 4 Hi byte = 'l' Word 4 Lo byte = 'e' Word 5 Hi byte = 'r' Word 5 Lo byte = ' ' Word 6 Hi byte = '\0' Word 6 Lo byte = '\0'
0x0030	20 words	ASCII	Product Name = "IE-SW-VL08M" Word 0 Hi byte = 'I' Word 0 Lo byte = 'E' Word 1 Hi byte = '-' Word 1 Lo byte = 'V' Word 2 Hi byte = 'L' Word 2 Lo byte = '0' Word 3 Hi byte = '8' Word 3 Lo byte = 'M' Word 4 Hi byte = '\0' Word 4 Lo byte = '\0'
0x0050	1 word		Product Serial Number
0x0051	2 words		Firmware Version Word 0 Hi byte = major (A) Word 0 Lo byte = minor (B) Word 1 Hi byte = release (C) Word 1 Lo byte = build (D)
0x0053	2 words	HEX	Firmware Release Date For example: Word 0 = 0 x 0609 Word 1 = 0 x 0705 Firmware was released on 2007-05-06 at 09 o'clock
0x0055	3 words	HEX	Ethernet MAC Address

			Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 04 Word 2 Lo byte = 0 x 05
0x0058	1 word	HEX	Power 1 0x0000: Off 0x0001: On
0x0059	1 word	HEX	Power 2 0x0000: Off 0x0001: On
0x005A	1 word	HEX	Fault LED Status 0x0000: No 0x0001: Yes
0x0082	1 word	HEX	DO1 0x0000: Off 0x0001: On
Port Information			
0x1000 to 0x1011	1 word	HEX	Port 1 to 8 Status 0x0000: Link down 0x0001: Link up 0x0002: Disable 0xFFFF: No port
0x1100 to 0x1111	1 word	HEX	Port 1 to 8 Speed 0x0000: 10M-Half 0x0001: 10M-Full 0x0002: 100M-Half 0x0003: 100M-Full 0xFFFF: No port
0x1200 to 0x1211	1 word	HEX	Port 1 to 8 Flow Ctrl 0x0000:Off 0x0001:On 0xFFFF:No port
0x1300 to 0x1311	1 word	HEX	Port 1 to 8 MDI/MDIX 0x0000: MDI 0x0001: MDIX 0xFFFF: No port
0x1400 to 0x1413 (Port 1) 0x1414 to 0x1427 (Port 2)	20 words	ASCII	Port 1 to 8 Description Port Description = “100TX,RJ45.” Word 0 Hi byte = ‘1’ Word 0 Lo byte = ‘0’ Word 1 Hi byte = ‘0’ Word 1 Lo byte = ‘T’ … Word 4 Hi byte = ‘4’ Word 4 Lo byte = ‘5’ Word 5 Hi byte = ‘.’ Word 5 Lo byte = ‘\0’
Packets Information			
0x2000 to 0x2023	2 words	HEX	Port 1 to 8 Tx Packets Ex: port 1 Tx Packet Amount = 44332211

			Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2100 to 0x2123	2 words	HEX	Port 1 to 8 Rx Packets Ex: port 1 Rx Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2200 to 0x2223	2 words	HEX	port 1 to 8 Tx Error Packets Ex: port 1 Tx Error Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2300 to 0x2323	2 words	HEX	port 1 to 8 Rx Error Packets Ex: port 1 Rx Error Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
Redundancy Information			
0x3000	1 word	HEX	Redundancy Protocol 0x0000: None 0x0001: RSTP 0x0002:Turbo Ring 0x0003:Turbo Ring V2 0x0004:Turbo Chain
0x3100	1 word	HEX	RSTP Root 0x0000: Not Root 0x0001: Root 0xFFFF: RSTP Not Enable
0x3200 to 0x3211	1 word	HEX	RSTP Port 1 to 8 Status 0x0000: Port Disabled 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: RSTP Not Enable
0x3300	1 word	HEX	TurboRing Master/Slave 0x0000: Slave 0x0001: Master 0xFFFF: Turbo Ring Not Enable
0x3301	1 word	HEX	TurboRing 1st Port status 0x0000: Port Disabled 0x0001: Not Redundant Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning

			0x0005: Forwarding
0x3302	1 word	HEX	TurboRing 2nd Port status 0x0000: Port Disabled 0x0001: Not Redundant Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005:Forwarding
0x3303	1 word	HEX	TurboRing Coupling 0x0000: Off 0x0001: On 0xFFFF: Turbo Ring is Not Enabled
0x3304	1 word	HEX	TurboRing Coupling Port Status 0x0000: Port Disabled 0x0001: Not Coupling Port 0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding 0xFFFF: Turbo Ring is Not Enabled
0x3305	1 word	HEX	TurboRing Coupling Control Port Status 0x0000: Port Disabled 0x0001: Not Coupling Port 0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding 0x0006: Inactive 0x0007:Active 0xFFFF:Turbo Ring is Not Enabled
0x3500	1 word	HEX	TurboRing V2 Coupling Mode 0x0000: None 0x0001: Dual Homing 0x0002: Coupling Backup 0x0003: Coupling Primary 0xFFFF:Turbo Ring V2 is Not Enabled
0x3501	1 word	HEX	TurboRing V2 Coupling Port Primary Status (Used in Dual Homing, Coupling Backup, and Coupling Primary) 0x0000:Port Disabled 0x0001: Not Coupling Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 is Not Enabled
0x3502	1 word	HEX	TurboRing V2 Coupling Port Backup Status (Only using in Dual Homing) 0x0000: Port Disabled 0x0001: Not Coupling Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 Not Enable

0x3600	1 word	HEX	TurboRing V2 Ring 1 status 0x0000: Healthy 0x0001: Break 0xFFFF:Turbo Ring V2 Not Enable
0x3601	1 word	HEX	TurboRing V2 Ring 1 Master/Slave 0x0000: Slave 0x0001: Master 0xFFFF: Turbo Ring V2 Ring 1 Not Enable
0x3602	1 word	HEX	TurboRing V2 Ring 1 1st Port Status 0x0000: Port Disabled 0x0001: Not Redundant Port 0x0002: Link Down 0x0003: Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Ring 1 is Not Enabled
0x3603	1 word	HEX	TurboRing V2 Ring 1's 2nd Port Status 0x0000: Port Disabled 0x0001: Not Redundant Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 Ring 1 is Not Enabled
0x3680	1 word	HEX	TurboRing V2 Ring 2 Status 0x0000: Healthy 0x0001: Break 0xFFFF: Turbo Ring V2 Ring 2 is Not Enabled
0x3681	1 word	HEX	TurboRing V2 Ring 2 Master/Slave 0x0000: Slave 0x0001: Master 0xFFFF: Turbo Ring V2 Ring 2 is Not Enabled
0x3682	1 word	HEX	TurboRing V2 Ring 2's 1st Port Status 0x0000: Port Disabled 0x0001: Not Redundant 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 Ring 2 is Not Enabled
0x3683	1 word	HEX	TurboRing V2 Ring 2's 2nd Port Status 0x0000: Port Disabled 0x0001: Not Redundant 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 Ring 2 is Not

			Enabled
0x3700	1 word	HEX	Turbo Chain Switch Roles 0x0000: Head 0x0001: Member 0x0002: Tail 0xFFFF: Turbo Chain is Not Enabled
0x3701	1 word	HEX	Turbo Chain 1st Port status 0x0000: Link Down 0x0001: Blocking 0x0002: Blocked 0x0003: Forwarding 0xFFFF: Turbo Ring V2 Ring 2 Not Enable
0x3702	1 word	HEX	Turbo Chain 2nd Port status 0x0000: Link Down 0x0001: Blocking 0x0002: Blocked 0x0003: Forwarding 0xFFFF: Turbo Ring V2 Ring 2 Not Enable

4.2 Profinet I/O

Introduction

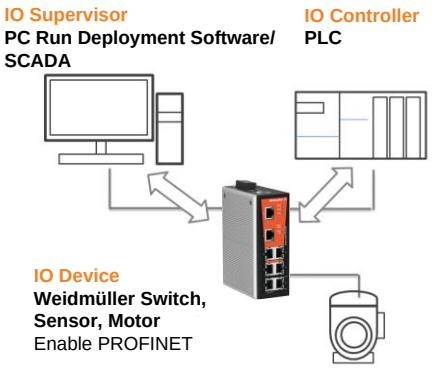
PROFINET is a communication standard for automation of PROFIBUS & PROFINET International (PI). It is 100% Ethernet-compatible as defined in IEEE standards. With PROFINET, applications can be implemented for production and process automation, safety applications, and the entire range of drive technology. With its integrated Ethernet-based communication, PROFINET satisfies a wide range of requirements, from data-intensive parameter assignment to extremely fast I/O data transmission.

PROFINET I/O is used for data exchange between I/O controllers (PLC, etc.) and I/O devices (field devices). This specification defines a protocol and an application interface for exchanging I/O data, alarms, and diagnostics. And its real-time (RT) solution allows response time in the range of 5 ms, which corresponds to today's PROFIBUS DP applications.

4.2.1 PROFINET Environmental Introductions

PROFINET Networking Structure

PROFINET I/O follows the Provider/Consumer model for data exchange. PROFINET forms logical link relationships between network character types. They are shown below.



There are 3 major character types defined by PROFINET I/O, including I/O controller, I/O supervisor, and I/O devices. Switches are considered I/O devices.

I/O Controller

This is typically the programmable logic controller (PLC) on which the automation program runs. The I/O controller provides output data to the configured I/O-devices in its role as provider and is the consumer of input data of I/O devices.

I/O Supervisor

This can be a programming device, personal computer (PC), or human machine interface (HMI) device for commissioning or diagnostic purposes.

I/O Device

An I/O device is a distributed I/O field device that is connected to one or more I/O controllers via PROFINET I/O. The I/O device is the provider of input data and the consumer of output data.

PROFINET I/O Devices

The Weidmüller switch is a PROFINET I/O device. A device model describes all field devices in terms of their possible technical and functional features. It is specified by the DAP (Device Access Point) and the defined modules for a particular device family. A DAP is the access point for communication with the Ethernet interface and the processing program.

PROFINET Protocols

DCP In PROFNET I/O, each field device has a symbolic name that uniquely identifies the field device within a PROFINET I/O system. This name is used for assigning the IP address and the MAC address. The DCP protocol (Dynamic Configuration Protocol) integrated in every I/O device is used for this purpose.

DHCP Because DHCP (Dynamic Host Configuration Protocol) is in widespread use internationally, PROFINET has provided for optional address setting via DHCP or via manufacturer-specific mechanisms.

PROFINET Type LLDP

Automation systems can be configured flexibly in a line, star, or tree structure. To compare the specified and actual topologies, to determine which field devices are connected to which switch port, and to identify the respective port neighbor, LLDP according to IEEE 802.1AB was applied in PROFINET I/O.

PROFINET filed bus exchange existing addressing information with connected neighbor devices via each switch port. The neighbor devices are thereby unambiguously identified and their physical location is determined.

Device descriptions

GSD file The GSD files (General Station Description) of the field devices to be configured are required for system engineering. This XML-based GSD describes the properties and functions of the PROFINET I/O field devices. It contains all data relevant for engineering as well as for data exchange with the device.

Refer to Appendix C how to get the GSDML file from the Weidmüller Internet Server.

4.2.2 Configuring PROFINET I/O on Weidmüller Switches

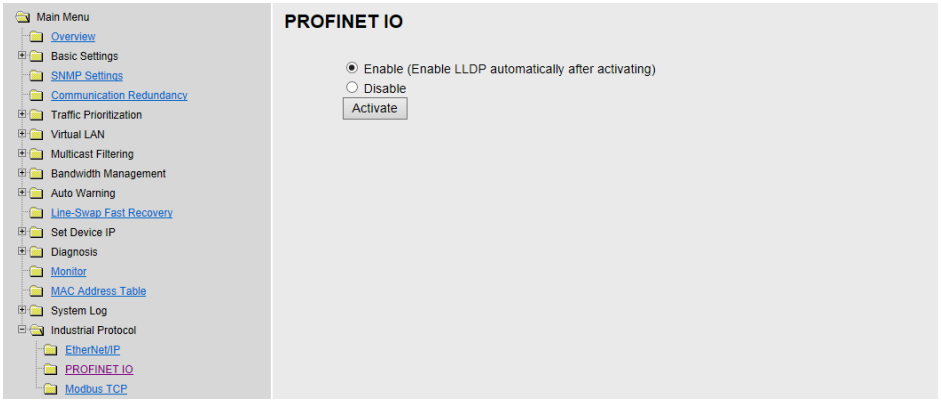
Enable PROFINET I/O in WEB UI on the Switch

The following steps show how to enable the Profinet I/O function on the Weidmüller switch:

1. Connect the configuration PC to the Switch
2. Change the IP address of the PC to one of the rang 192.168.1.0 / 24

   e.g. IP address 192.168.1.200 / Subnet mask 255.255.255.0
3. Start a Web browser and log into the Web interface of the Switch (default IP address of the switch is 192.168.1.110)

   Username: admin / Password: Detmold
4. Select menu **Industrial Protocol** -> **PROFINET IO**



5. Select **Enable** option and click **Activate** to enable PROFINET I/O.

The PROFINET type LLDP will be enabled automatically when PROFINET I/O is enabled. Select the **Disable** option and click **Activate** to disable PROFINET I/O.

The switch will disable PROFINET type LLDP and will use then standard LLDP.

PROFINET I/O functionality is implemented in firmware version 3.3.x and later.

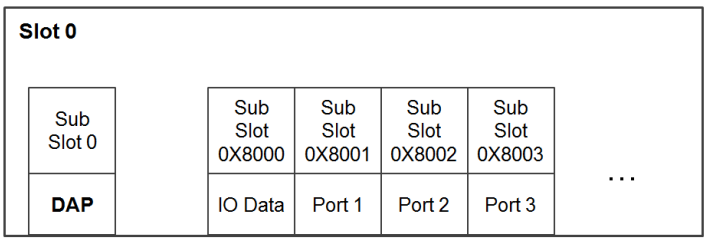
If you use a managed Switch with firmware version 2.x you can update the firmware to latest version 3.3.x. Your hardware already is capable to run the industrial protocols.

By factory default the PROFINET I/O functionality is disabled (all Weidmüller managed Switches).

4.2.3 Step 7 Integration

Addressing of I/O Data in PROFINET I/O Based on Slot and Sub-Slots

The concept of the Weidmüller PROFINET switch with GSD version 2 is shown the table below. In this structure, each switch port represents one sub-slot.



Manufacturer Information

Each PROFINET device is addressed based on a MAC address. This address is unique worldwide. The company code (bits 47 to 24) can be obtained from the IEEE Standards Department free of charge. This part is called the OUI (organizationally unique identifier).

Table of Weidmüller OUI

Bit Value 47..24						Bit Value 23..0					
0	0	1	5	7	E	x	x	x	x	x	x
Company Code (OUI)						Consecutive Number					

4.2.4 Overview of Operation Procedure

The following steps show how to integrate the switch into a PROFINET network:

1. Activate PROFINET protocol on the switch

→ Enable checkbox PROFINET in switch web UI

2. Create a PROFINET I/O subnet project in STEP 7

→ Create a PROFINET I/O Ethernet project for deploying environment

3. GSD file installation

→ Import Weidmüller switch GSD into the project

4. Device configuration

→ Search and discover the switch in STEP 7. Configure PROFINET attributes such as IP address, device name and I/O parameters.

5. Save and load the project into the PLC

→ Load this project and save into the PLC

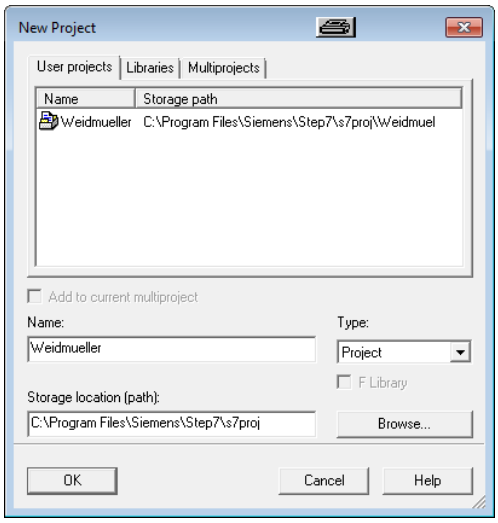
6. Monitoring the Switch

→ Use STEP 7 to monitor switch attributes

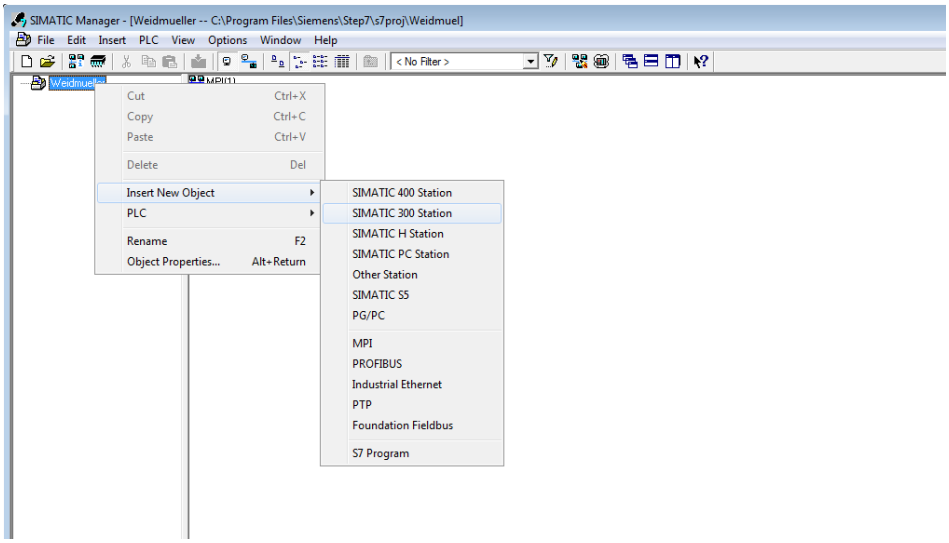
4.2.5 Create a PROFINET I/O Subnet Project

Start SIMATIC Manager, click file in the menu bar > New Project

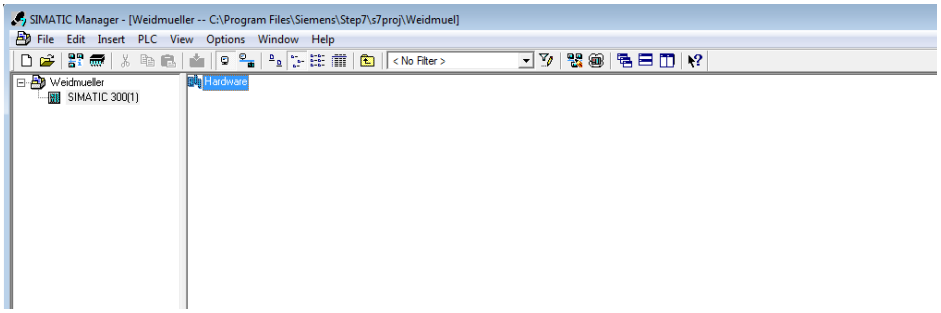
Name your project in the **Name** field then click **OK.**



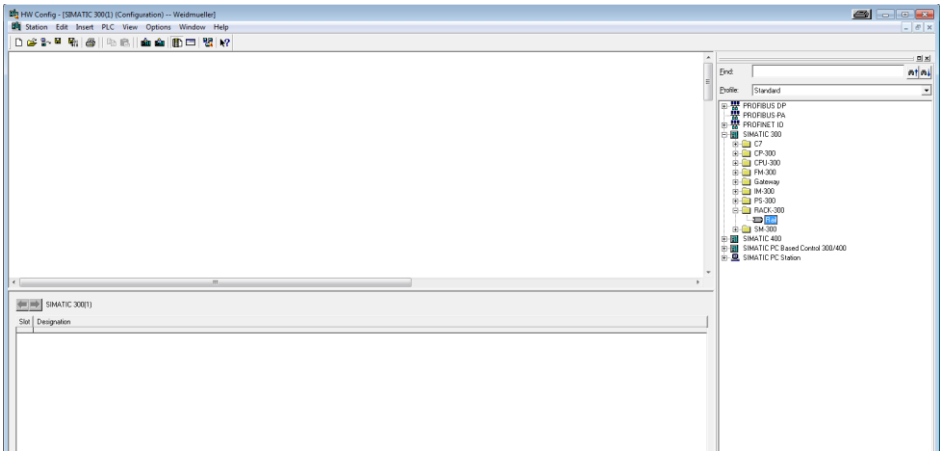
Insert a station in your project by...
Right click in category column > Insert New Object > your PLC series (here we select SIMATIC 300 station).



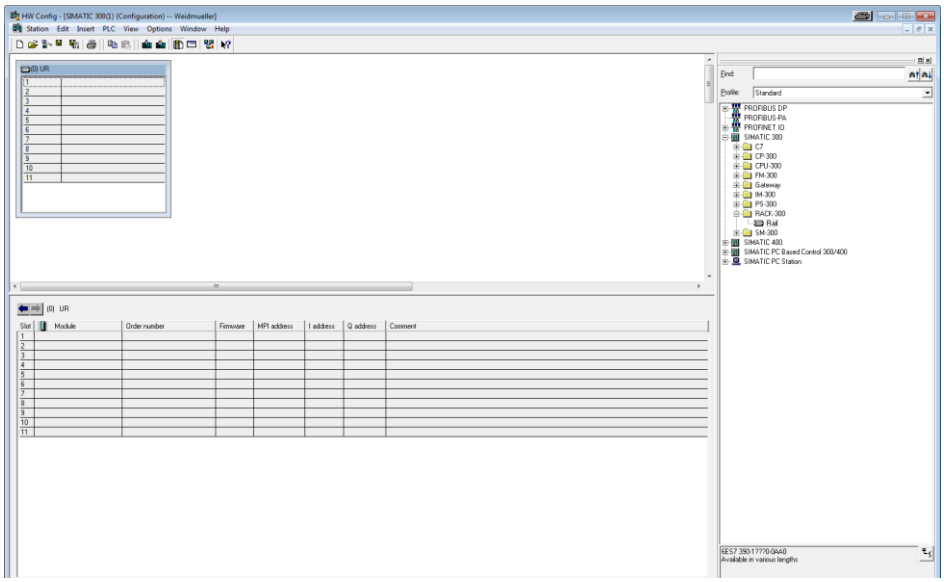
Then you can see the new object in the project. Double click on the **Hardware**.



After double-clicking on HW, you will see the **HW Config** window.

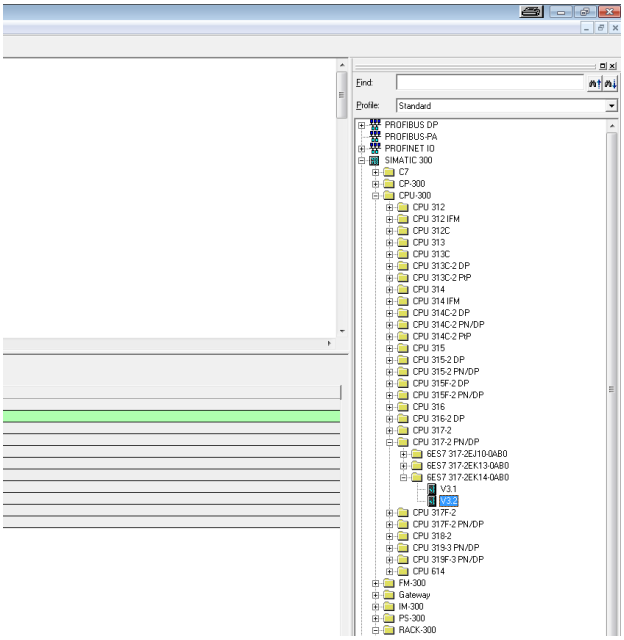


Drag a rack from the side bar to main dashboard. Click **Rack-300** and drag **Rail** to the main screen.

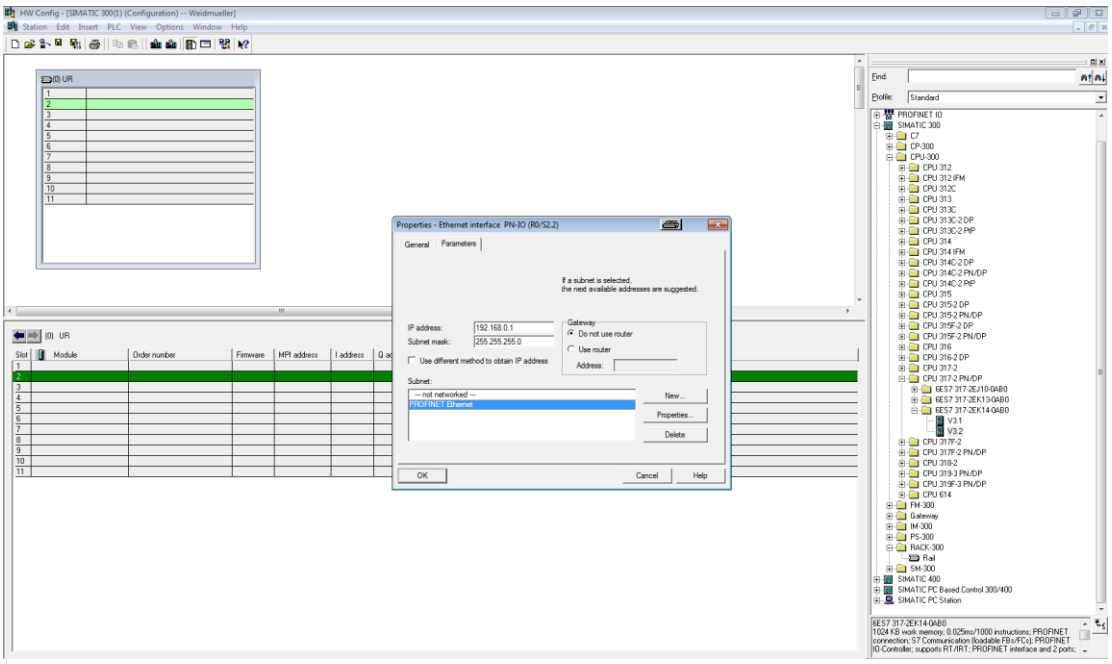


Add PLC CPU in HW Config

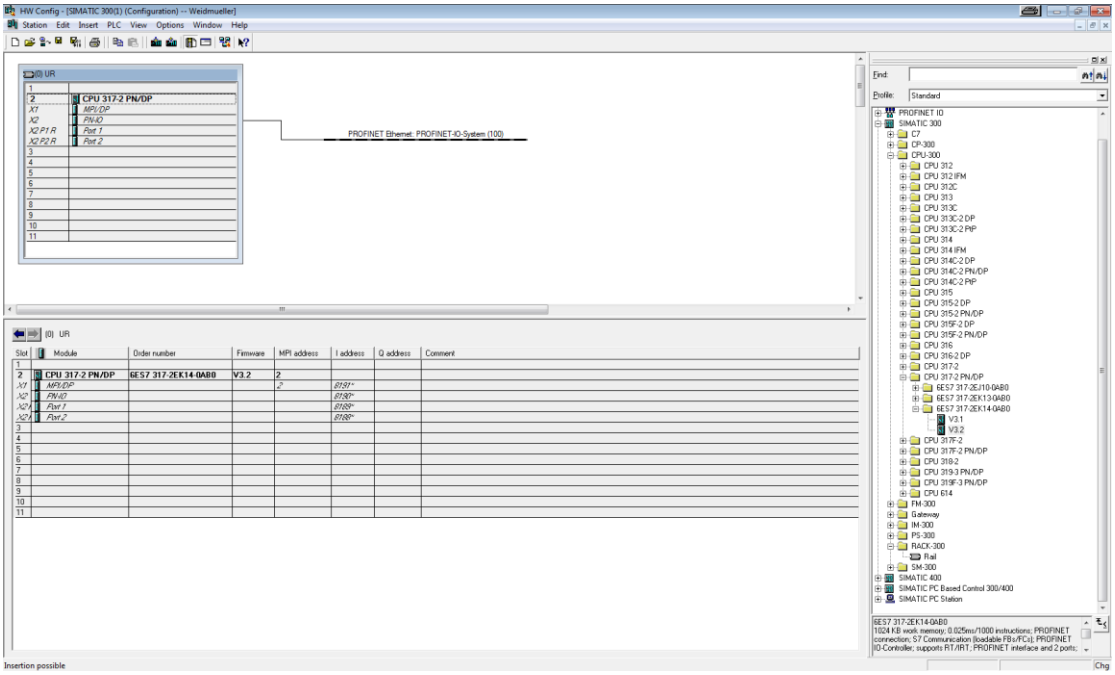
Select your PLC CPU and drag it to the rack slot 2. Please select by PLC you used. Here we will select 6ES7-317-2EK14-0AB0 V3.2.



Now, the Ethernet interface dialog will pop out. Fill your PLC **IP address** in “IP address” column. Then click **New** in subnet to create a new Ethernet subnet. Here we will create a subnet named “PROFINET Ethernet”, then click **OK.**

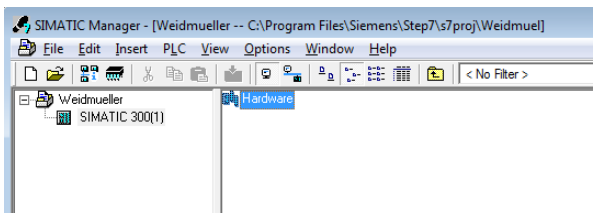


PROFINET I/O Ethernet subnet project now is accomplished.



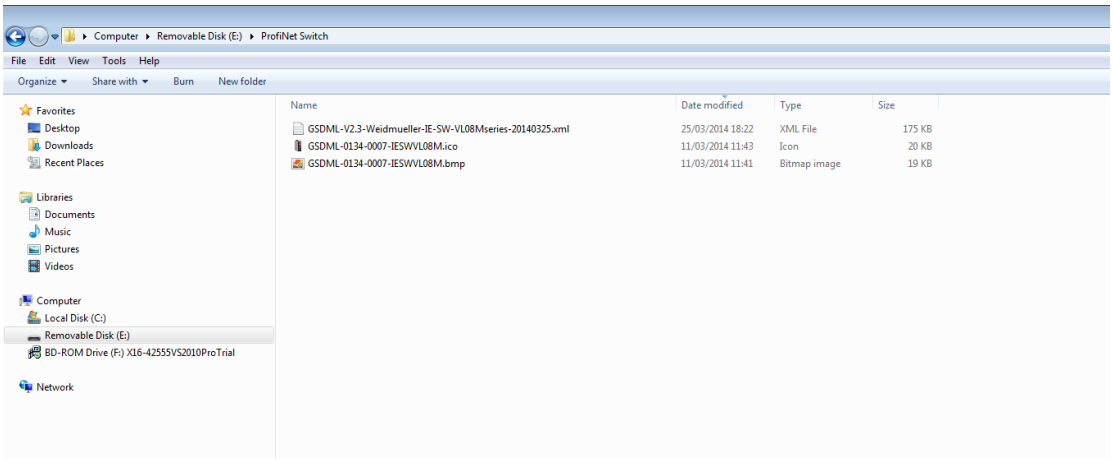
4.2.6 GSD File Installation

1. Start SIMATIC manager on your PC.
2. Open your project.
3. Open hardware configuration.

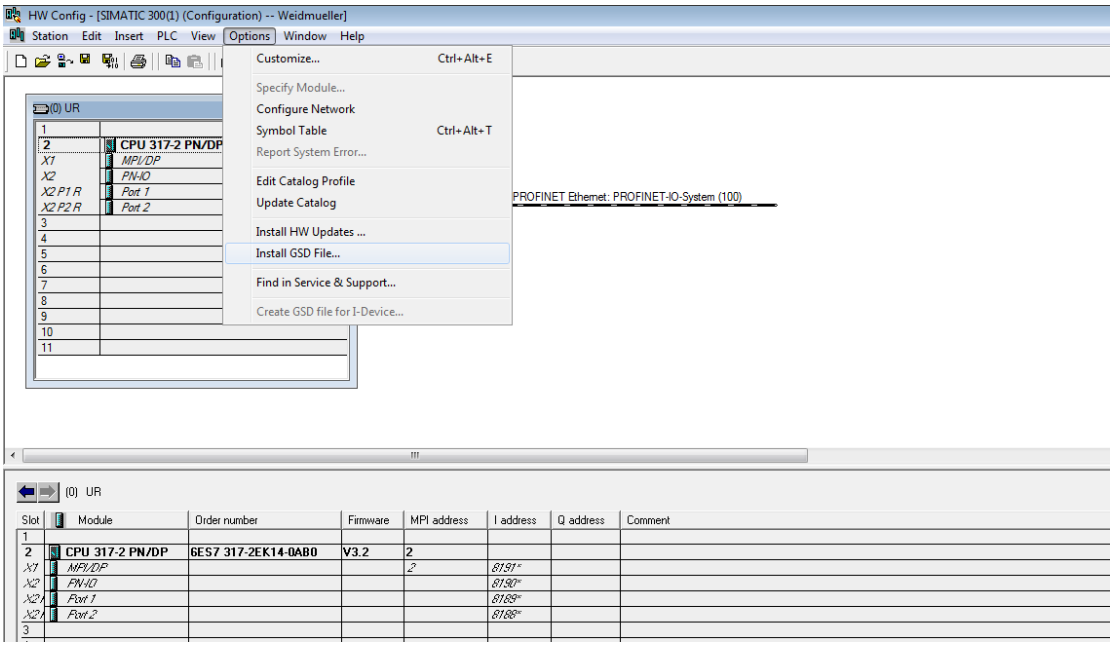


Installing the GSD file

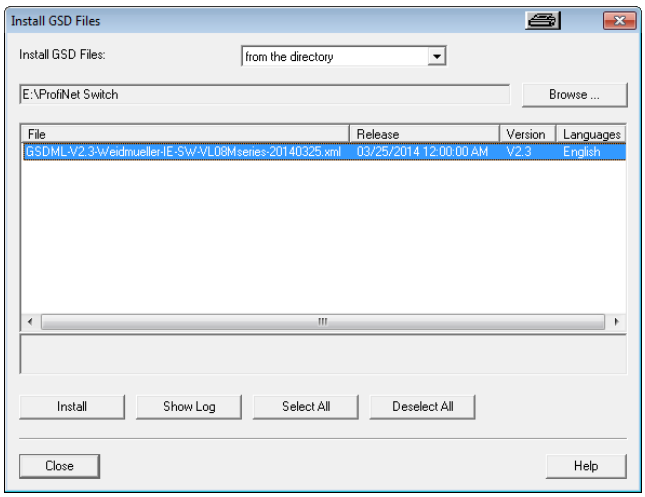
4. Put the GSD file and icon file on your PC at the same folder.



5. Click **Options** > **Install GSD File**



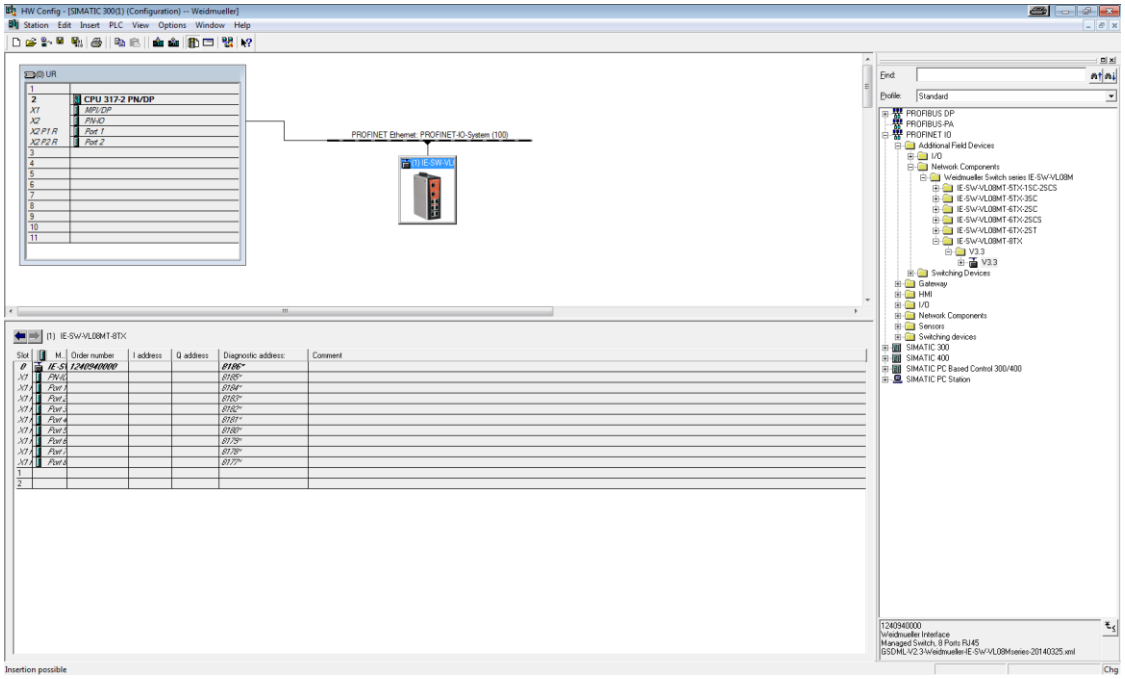
6. Click button **Browse...** to select the GSD file and click **Install**



When the GSD file successfully is installed, you will find Weidmüller switches in the side bar under:

PROFINET IO > Additional Field Devices > Network Components > Weidmueller Switch series

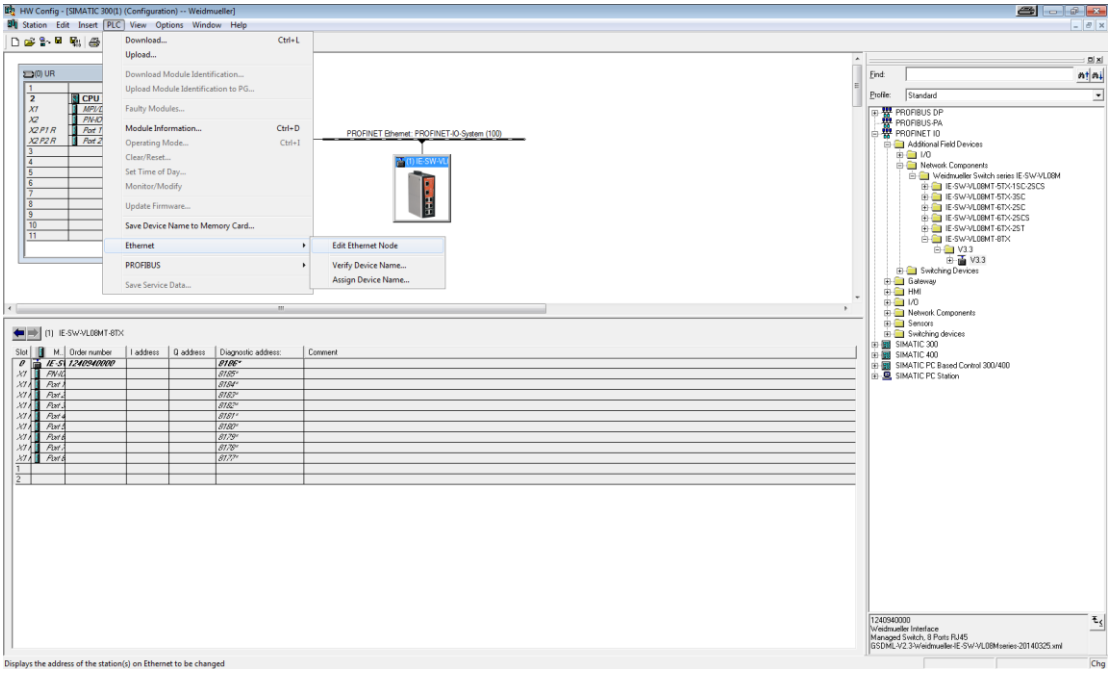
7. Select the Weidmüller switch from the side bar (in this case V3.3) and use Drag & Drop to pull the switch onto the bus cable. Then you can see the Weidmüller switch icon displayed on the screen.



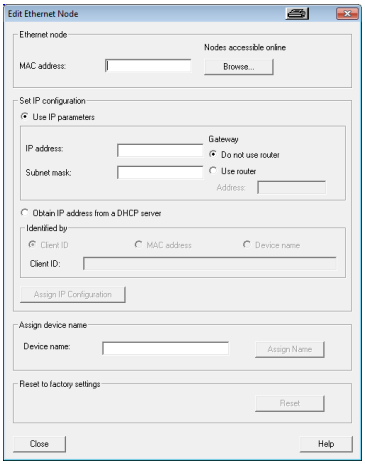
4.2.7 Device Configuration

Browse the switch

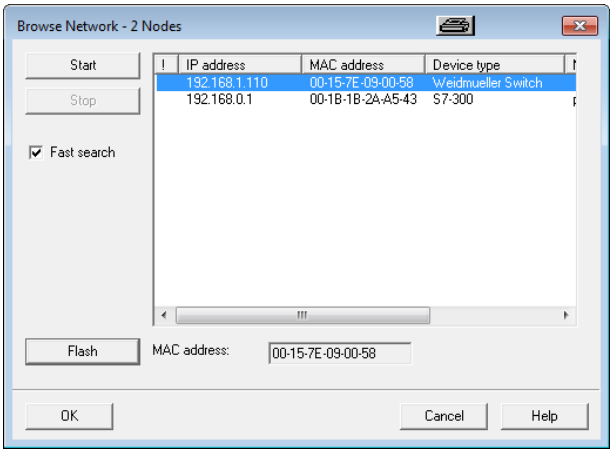
1. Select **PLC** > **Ethernet** > **Edit Ethernet node** to open the Browse dialog.



2. When the **Edit Ethernet Node** dialog box appears, click **Browse**



3. Select your target switch and click **OK**



4. Assign IP address and Device name to the switch

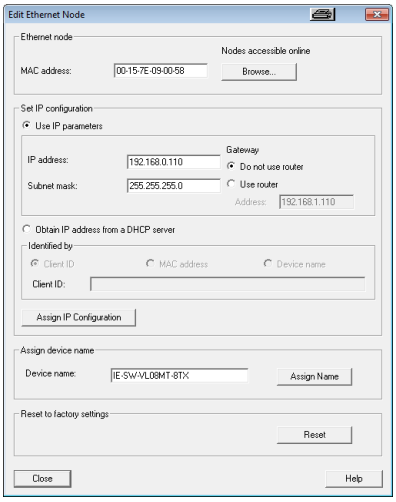
→ Give the switch an IP address and subnet mask (e.g. 192.168.0.110, 255.255.255.0)

→ Click **Assign IP configuration**

→ Give the switch a name (e.g. IE-SW-VL08MT-8TX)

→ Click **Assign Name**

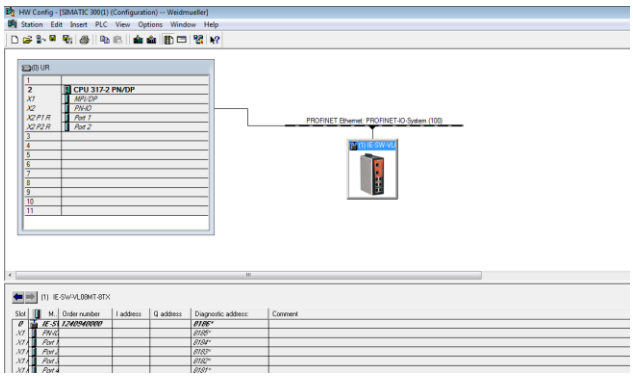
→ Click **Close** to finish



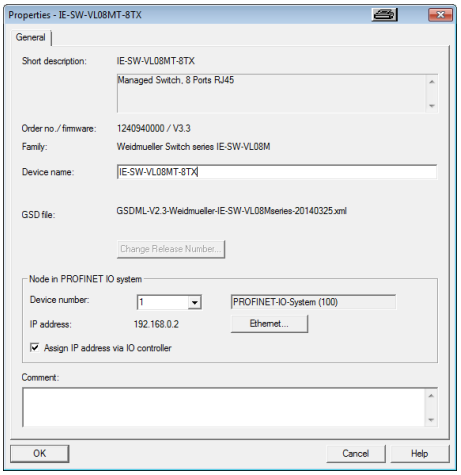
NOTE The field **Device name** does not allow any empty spaces in the name. If the device name is entered with a space, the system will remove words after the space automatically.

5. Set IP address and device name in your project

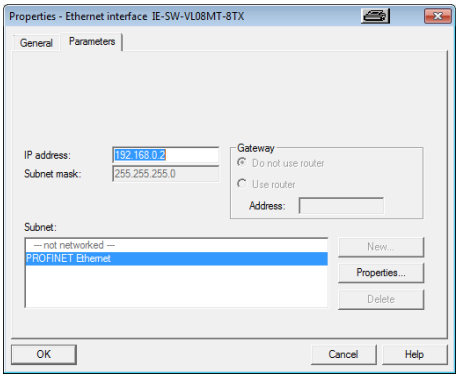
→ Double-click the switch icon to open switch property menu.



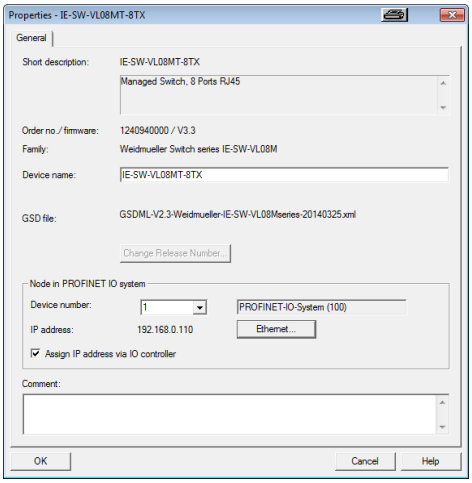
→ Set the **Device name** corresponding with those you have just assigned under section "**Edit Ethernet Node"**. (e.g. IE-SW-VL08MT-8TX)



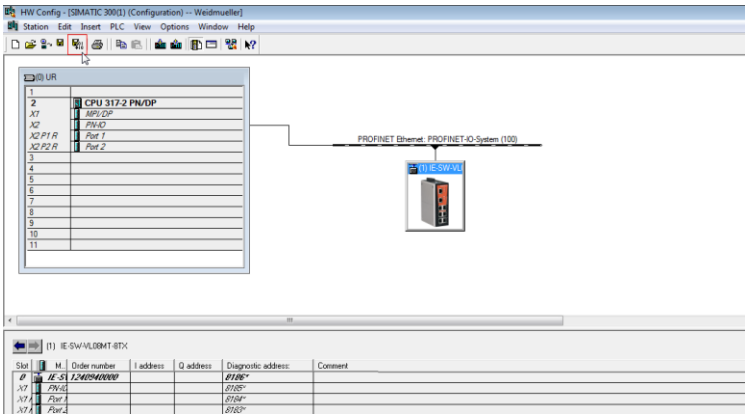
→ Click **Ethernet…** and set manually the **IP address** corresponding with those you have just assigned in STEP 7 (e.g. 192.168.0.110)



→ Then click **OK**

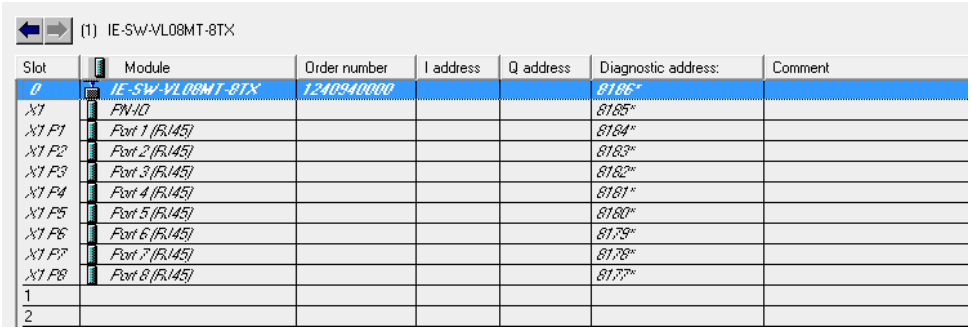


6. Click **Save and Compile** in the Hardware configuration.



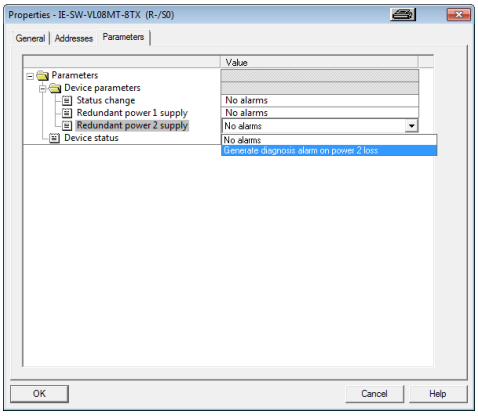
4.2.8 Configuring device properties

1. Select the switch and double-click the first sub-module slot 0 to set device properties.



2. Select **Parameters** and change the device parameter settings.

3. Click Save and Compile

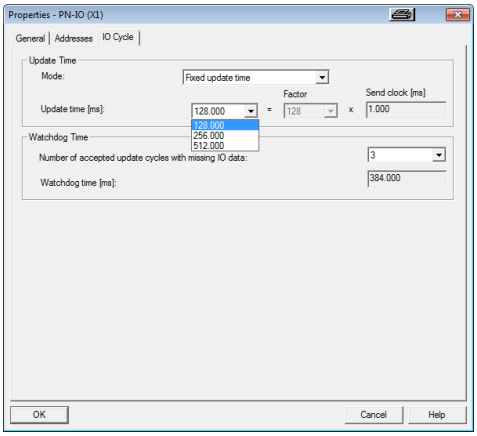


Configuring I/O cycle time

1. Select the switch and double-click the **sub-module X1** to set the I/O cycle.

2. Select **IO Cycle** and change the I/O cycle settings.

3. Click Save and Compile.

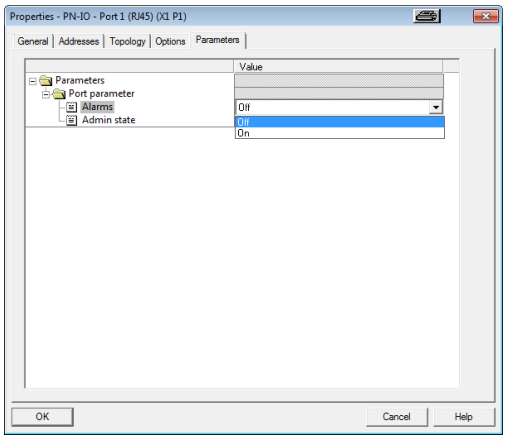


Configuring port property

1. Select the switch and double-click the **sub-module X1 P1** to set port property for Port 1.

2. Select **Parameters** and change the port parameters settings.

3. Click **Save and Compile**

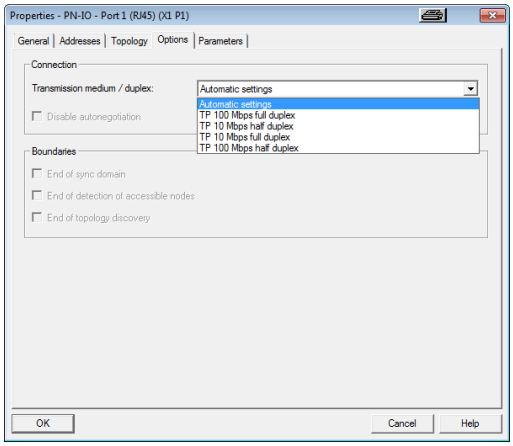


Configuring connection options

1. Select the switch and double-click the **sub-module X1 P1** to set port options for Port 1.

2. Select **Options** and change the port option settings.

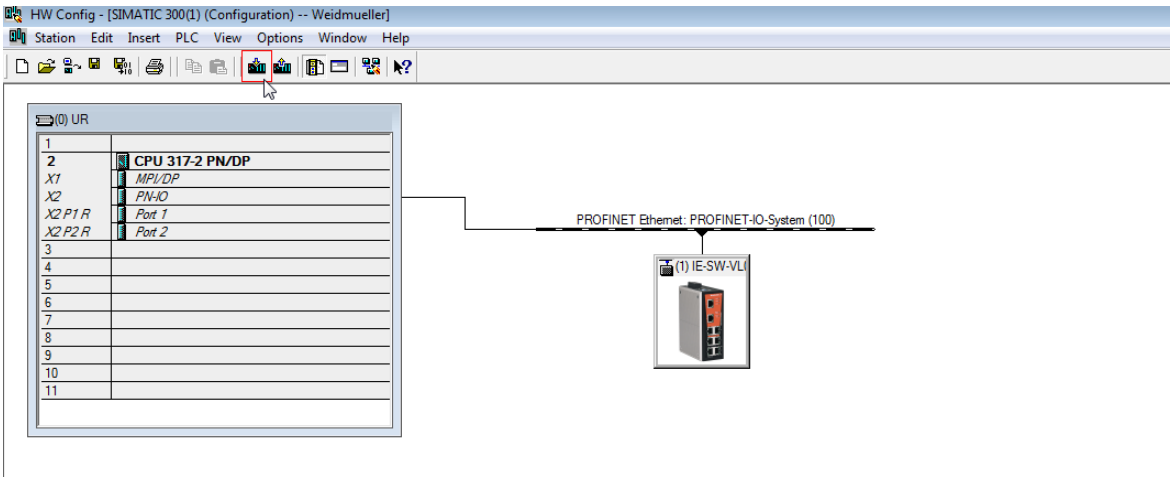
3. Click **Save and Compile**



4.2.9 Download the Project into the PLC

When the configuration is already saved and compiled, then click the icon (in red box) to download project configuration to the PLC.

After the project is configured, SIMATIC STEP 7 will load all information required for data exchange to the I/O Controller (PLC), including the IP addresses of the connected I/O devices.



4.2.10 Monitoring the Switch

PROFINET Attributes

The PROFINET I/O connection can be configured for both cyclic I/O data and I/O parameters. I/O parameters are acyclic I/O data. These are major setup and monitor attributes in PROFINET.

Cyclic I/O Data
Cyclic I/O data are always sent between the PLC and Switches at the specified periodic time. These data are transmitted almost real time. For example, status information from the Switches, and variables to be written to the Switch would typically be part of the cyclic data.

I/O Parameters
PROFINET I/O parameters are defined for device configuration and status monitoring. These data are useful for infrequent data transfers, or for very large data transfers. Only transfer when needed

Alarm

Alarms are mainly PROFINET I/O transmitted high-priority events. Alarm data are exchanged between an I/O device and an I/O controller. Once an event triggers it, the switch will send the alarm to the PLC immediately. Enable or disable these alarms by setting I/O parameters.

PROFINET Cyclic I/O Data

The Weidmüller switch provides PROFINET I/O cyclic data as described in below table.

NOTE: The default transfer frequency of the Switch's *PROFINET Cyclic I/O data* is 128 ms. There are 3 options available in SIMATIC STEP 7: 128 / 256 / 512 ms.

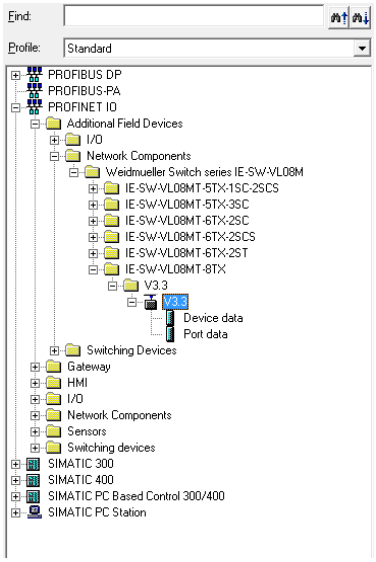
PROFINET Cyclic I/O Data Table

Category	Direction	Byte	Bit	Name	Description
Device	Input	0	0	Device status	0 is failed status, 1 is OK.
			1	Power 1	0 is unavailable, 1 is OK
			2	Power 2	0 is unavailable, 1 is OK
			3	RSTP status	0 is disabled, 1 is enabled
			4	Turbo Ring v1	0 is disabled, 1 is enabled
			5	Turbo Ring v2	0 is disabled, 1 is enabled
			6	Turbo Chain	0 is disabled, 1 is enabled
			7	Turbo Ring v2 status	0 is broken, 1 is healthy
Port	Input	1	0	Port 1 Connection	0 is not connected, 1 is connected
			1	Port 2 Connection	0 is not connected, 1 is connected
			2	Port 3 Connection	0 is not connected, 1 is connected
			3	Port 4 Connection	0 is not connected, 1 is connected
			4	Port 5 Connection	0 is not connected, 1 is connected

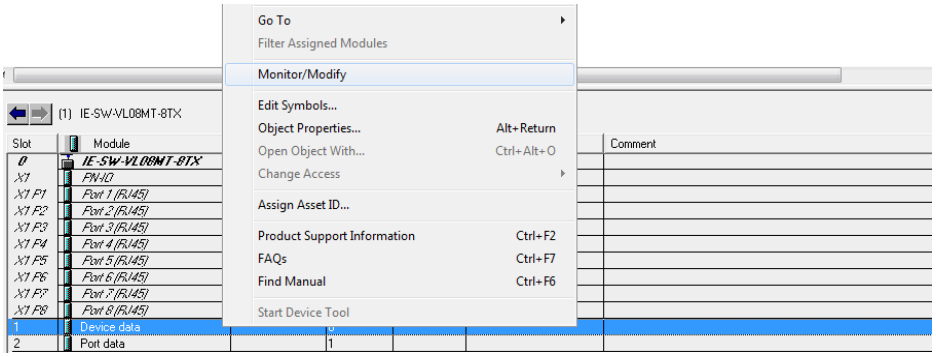
			5	Port 6 Connection	0 is not connected, 1 is connected
			6	Port 7 Connection	0 is not connected, 1 is connected
			7	Port 8 Connection	0 is not connected, 1 is connected

Monitor PROFINET I/O Cyclic Data

Weidmüller switches provide PROFINET I/O cyclic data for real-time monitoring. In side bar you can see **Device data** and **Port data.**

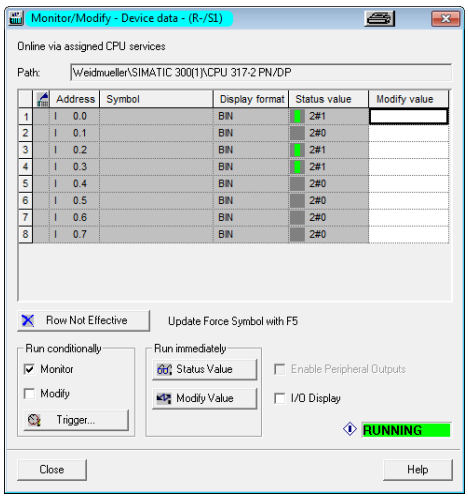


To monitor Device data, use Drag & Drop to pull the **Device data** onto **slot 1**. Right-click on slot 1, then select **Monitor/Modify**.



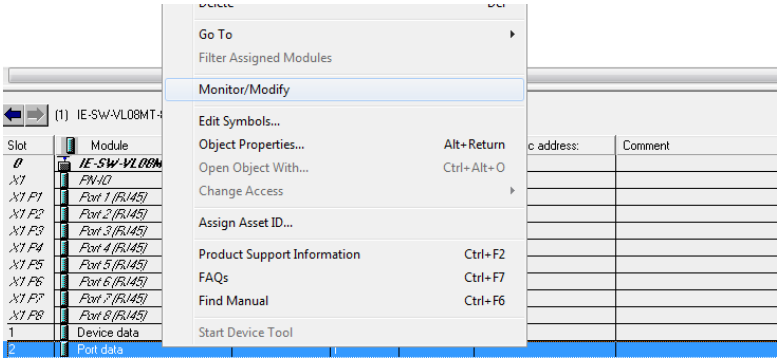
Use Monitor to check the input data value. In this dialog, select **Monitor** and then, you can see the status value of each address. Please refer to the **PROFINET Cyclic I/O data table** to see the meaning of each bit.

For example, address 0.2 is set to Bit 1. It represents Power 2 status of the switch. 1 means Power 2 is present and **Green** will be displayed in the section **Status value.**



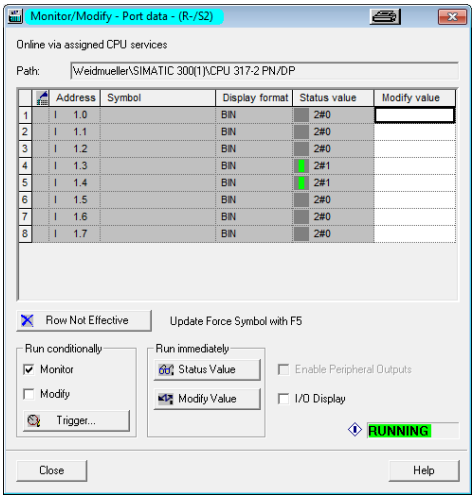
Refer to the **PROFINET Cyclic I/O data table** at the beginning of this chapter for the meanings of each address.

To monitor Port data, follow the same steps, drag **Port data** in the side bar and drop it onto **slot 2**.



Then right click on slot 2 and select **Monitor/Modify.** You will see a monitoring window. Please refer to the **PROFINET Cyclic I/O data table** to see the meaning of each bit.

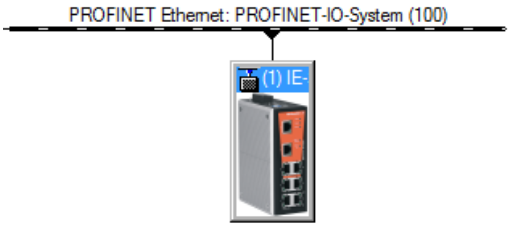
For example, address 1.3 is set to Bit 1. It represents the connection status of Port 4 of the switch. Bit 1 means that a connection is present at Port 4 and **Green** will be displayed in the section **Status value.**

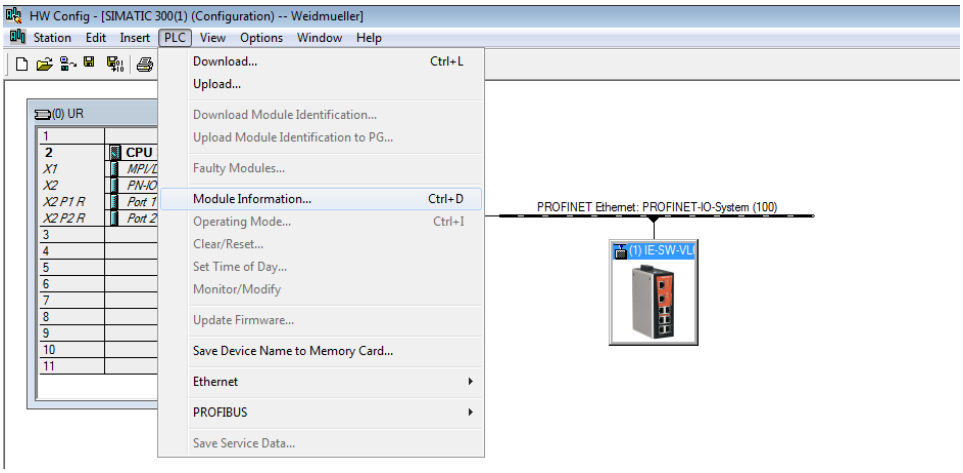


Module Information

Weidmüller switches support SIMATIC STEP 7 Ethernet traffic information monitoring and PROFINET alarms. These attributes can be monitored in module information dialog. Following are the steps of operation.

1. Select Weidmüller switch icon in the HW config.
2. Click menu bar **PLC** > **Module Information**



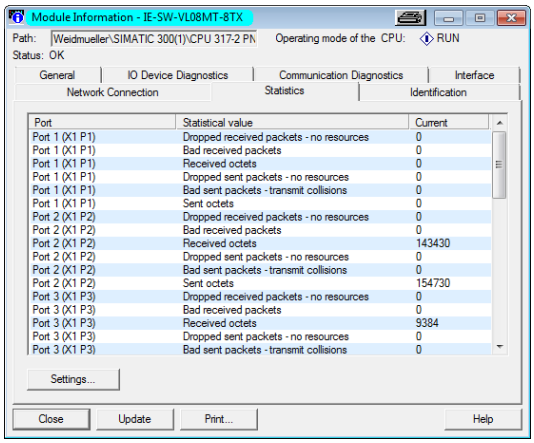


The module information dialog will then pop up.

Port Statistics Output

Select **Statistics** tab. Find out each port traffic information list below.

The Statistics tab lists each port traffic status and the number of packets. Click **Update** to refresh the data.

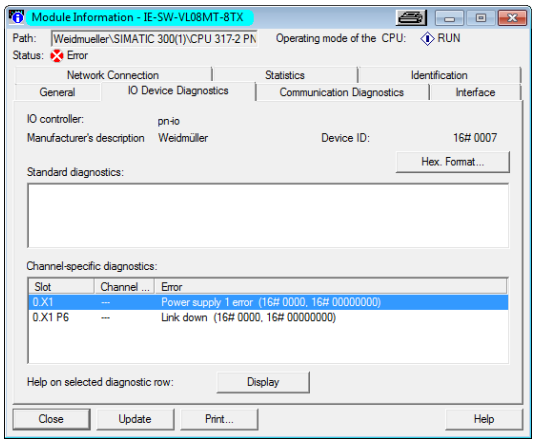

Module Information - IE-SW-VL08MT-8TX
Path: Weidmueller\SIMATIC 300(1)\CPU 317-2 PN
Operating mode of the CPU: RUN
Status: OK
General
IO Device Diagnostics
Communication Diagnostics
Interface
Network Connection
Statistics
Identification
Port
Statistical value
Current
Port 1 (X1 P1) Dropped received packets - no resources 0
Port 1 (X1 P1) Bad received packets 0
Port 1 (X1 P1) Received octets 0
Port 1 (X1 P1) Dropped sent packets - no resources 0
Port 1 (X1 P1) Bad sent packets - transmit collisions 0
Port 1 (X1 P1) Sent octets 0
Port 2 (X1 P2) Dropped received packets - no resources 0
Port 2 (X1 P2) Bad received packets 0
Port 2 (X1 P2) Received octets 143430
Port 2 (X1 P2) Dropped sent packets - no resources 0
Port 2 (X1 P2) Bad sent packets - transmit collisions 0
Port 2 (X1 P2) Sent octets 154730
Port 3 (X1 P3) Dropped received packets - no resources 0
Port 3 (X1 P3) Bad received packets 0
Port 3 (X1 P3) Received octets 9384
Port 3 (X1 P3) Dropped sent packets - no resources 0
Port 3 (X1 P3) Bad sent packets - transmit collisions 0
Settings...
Close
Update
Print...
Help

4.2.11 I/O Device Diagnostics

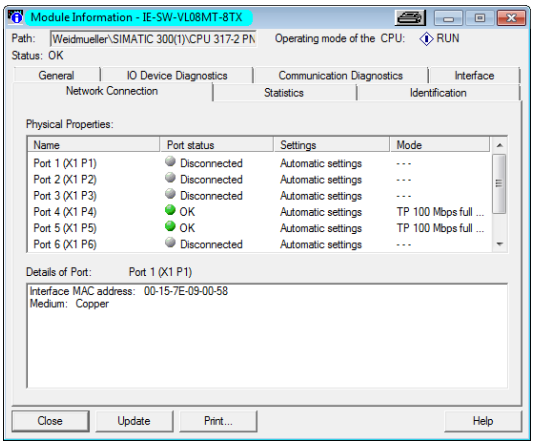
Weidmüller PROFINET switches support PROFINET alarms. These alarm messages will be sent by the switch immediately when an event is triggered. These alarms can be enabled/disabled using PROFINET I/O parameters (see chapter **PROFINET I/O Parameters**).

Select **IO Device Diagnostics** tab to view alarms received by the PLC.

The **Channel-specific diagnostics** field is displaying link-down alarm information. Click **Update** to refresh the data.

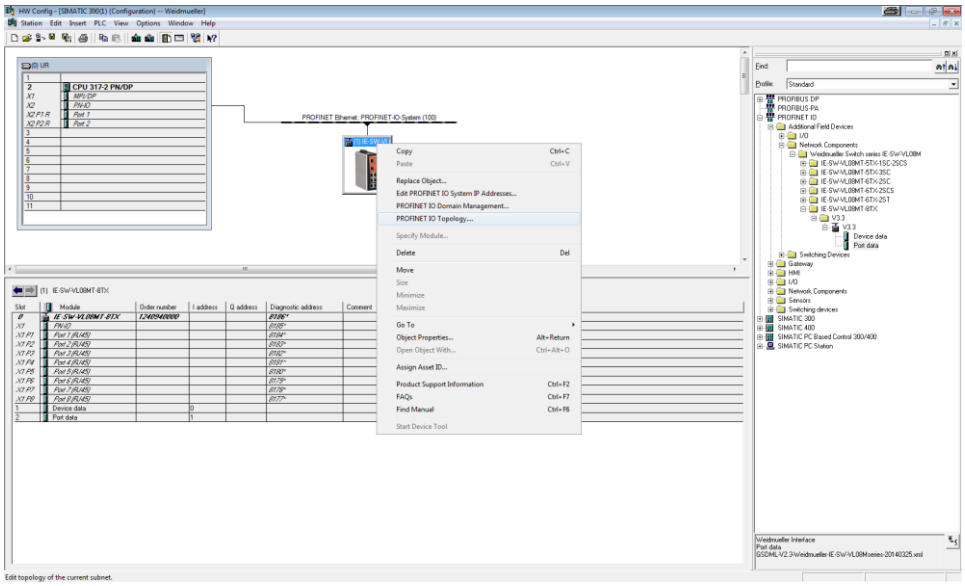


Select **Network Connection Diagnosis** tab to view the connection status.

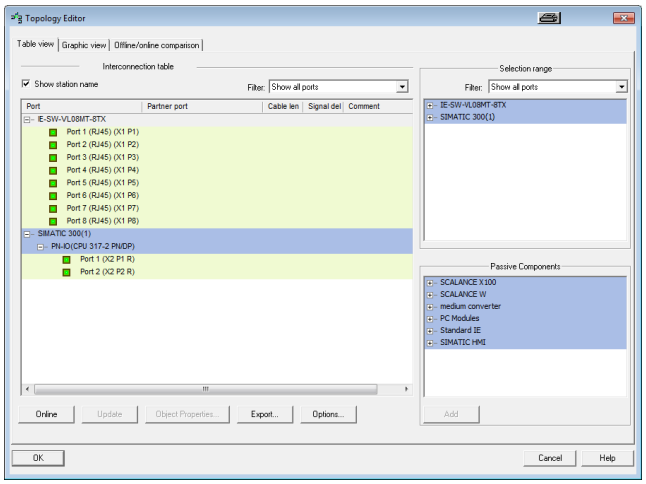


4.2.12 Topology Editor

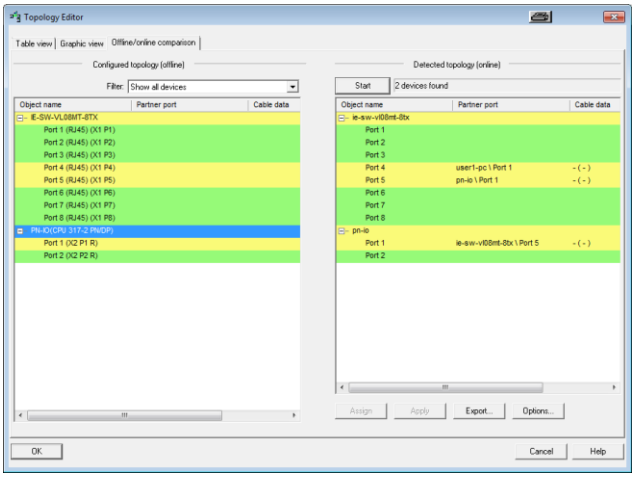
Weidmüller switches support SIMATIC STEP 7 Topology editor. Select Weidmüller switch Icon on the screen, then right click on **PROFINET IO Topology**.



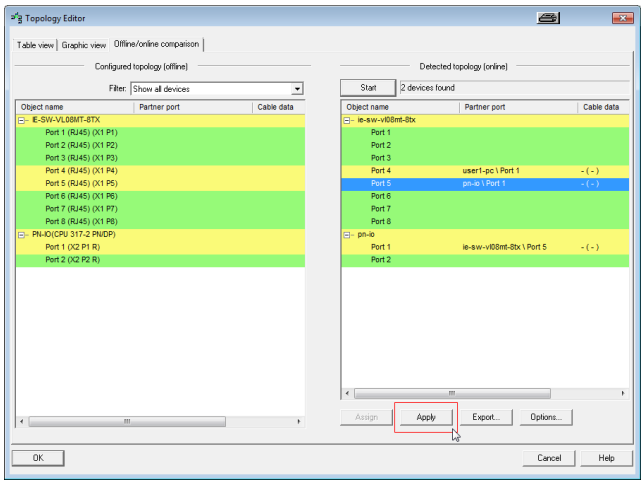
All port's status will be displayed in **table view** tab.



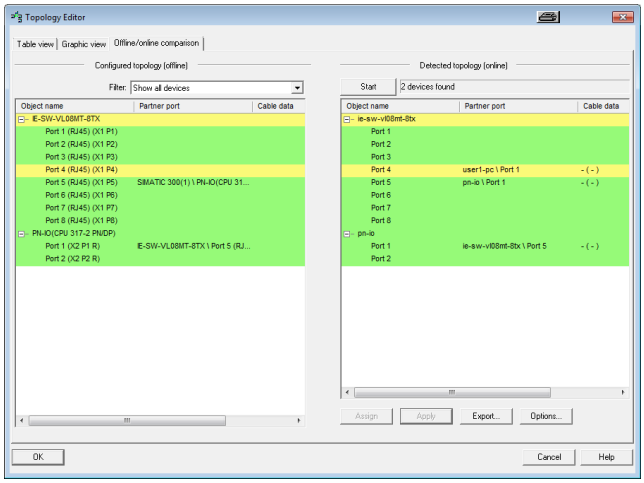
In the **Offline/Online Comparison** tab, you can compare device partner ports. Click S**tart** to discover connection relationships.



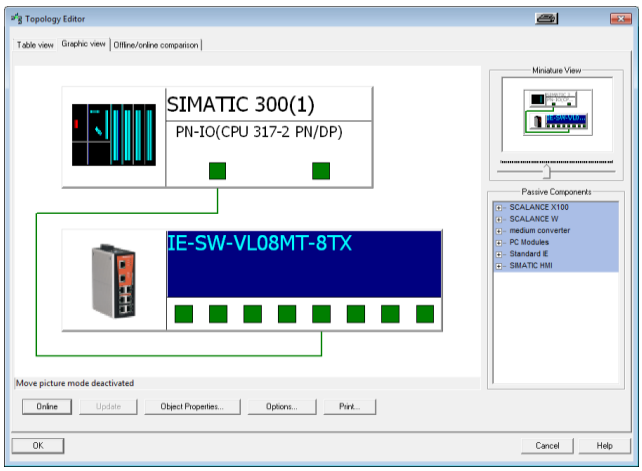
Select the every connected port in the online topology window and click **Apply** button to confirm the device partner ports.



After compared devices partner ports in the **Offline/Online Comparison** tab, click **Graphic view** to display the network topology.



You can also draw the connection of each port manually in **Graphic view** tab.



4.2.13 PROFINET I/O Parameters

Weidmüller defines comprehensive PROFINET I/O parameters for more flexible settings and monitoring. There attributes are readable or writable. PROFINET I/O parameters use PROFINET acyclic data to achieve communication in the network. You can use the SIMATIC STEP 7 tool or engineering deployment software to edit it. There are 3 categories of parameters, including Device Parameters, Device Status and Port Parameters. The following tables provide parameter information:

rw: Read and Write

ro: Read Only

Device parameters

These parameters control PROFINET Alarm functions. PROFINET Alarm is a message which sends from switch to PLC immediately once the event is triggered.

Byte	Name	Access	Value	Description	Default Value
0	Status Alarm	rw	0	Do not send any alarms	0: No alarms
			1	Send alarm if any status change	
1	Power Alarm 1	rw	0	Do not send power failed alarms	0: No alarms
			1	Send alarm if power supply 1 fails	
2	Power Alarm 2	rw	0	Do not send power failed alarms	0: No alarms
			1	Send alarm if power supply 2 fails	

Device Status

Byte	Name	Access	Value	Description
0	Device Status	ro	0	Unavailable
			1	OK
			2	Device bootup fails
1	Fault Status	ro	0	Unavailable
			1	OK
			2	Device detect fault
2	Power 1 Status	ro	0	Unavailable
			1	OK
			2	Power 1 fails
3	Power 2 Status	ro	0	Unavailable
			1	OK
			2	Power 2 fails

4	DI 1 Status	ro	0	Unavailable
			1	Closed
			2	Open
5	DI 2 Status	ro	0	Unavailable
			1	Closed
			2	Open
6	Redundant Mode	ro	0	Unavailable
			1	RSTP
			2	Turbo Ring V1
			3	Turbo Ring V2
			4	Turbo Chain
7	Ring Status	ro	0	Unavailable
			1	Healthy
			2	Break
8	Redundant Port 1 Status	ro	0	Unavailable
			1	Link is up
			2	Link is down
9	Redundant Port 2 Status	ro	0	Unavailable
			1	Link is up
			2	Link is down
10	Ring Coupling Mode	ro	0	Unavailable
			1	Backup
			2	Primary
			3	Dual homing
11	Coupling Port 1 Status	ro	0	Unavailable
			1	Link is up
			2	Link is down
12	Coupling Port 2 Status	ro	0	Unavailable
			1	Link is up
			2	Link is down
13	Connection	ro	0	Unavailable
			1	OK
			2	Connection failure

Port Parameters

Byte	Name	Access	Value	Description
0	Port Alarm	rw	0	Do not send alarm
			1	Send alarm when port link down
1	Port Admin State	rw	0	Unavailable
			1	Off

			2	On
2	Port Link State	ro	0	Unavailable
			1	Link is up
			2	Link is down
3	Port Speed	ro	0	Unavailable
			1	10
			2	100
			3	1000
4	Port duplex	ro	0	Unavailable
			1	Half
			2	Full
5	Port Auto-negotiation	ro	0	Unavailable
			1	Off
			2	On
6	Port flow control	ro	0	Unavailable
			1	Off
			2	On
7	Port MDI/MDIX	ro	0	Unavailable
			1	MDI
			2	MDIX

A. Weidmüller Switch Configuration Utility

The Weidmüller switch configuration utility (WM_Switch_Utility.exe) is a comprehensive Windows-based GUI that can be used to configure and maintain multiple Weidmüller managed switches.

A suite of useful functions is available to help you

- to locate Weidmüller switches which are attached to the same LAN as the PC host (regardless of whether or not you know the IP addresses of the switches)
- to connect to an Weidmüller switch whose IP address is known
- to modify the network configurations of one or multiple Weidmüller switches
- and to update the firmware of one or more Weidmüller Switches.

The Weidmüller Switch Configuration Utility is designed to provide you with instantaneous control of your Weidmüller Switches regardless of location. You may download the Weidmüller Switch Configuration Utility software from Weidmüller's website free of charge.

The following topics are covered in this chapter:

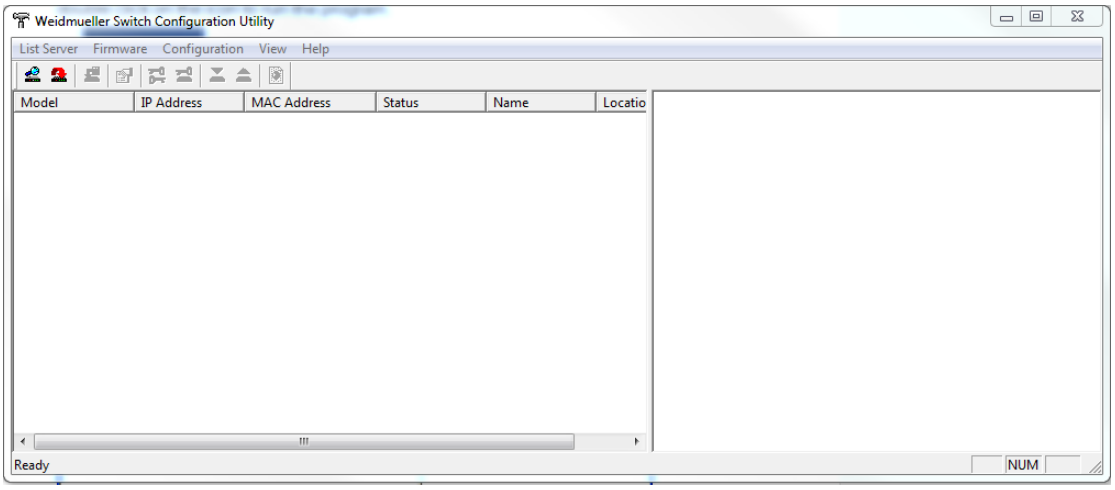
- **Starting Weidmüller Switch Configuration Utility**
- **Broadcast Search**
- **Search by IP Address**
- **Unlock the Ethernet Switch**
- **Upgrade Firmware**
- **Modify IP Address**
- **Export Configuration**
- **Import Configuration**

A1.1 Starting Weidmüller Switch Configuration Utility

To start the Weidmüller Switch Configuration Utility, locate and then run the executable file **WM_Switch_Utility.exe**.

For example, if the file was placed on the Windows desktop, it should appear as follows. Simply double click on the icon to run the program.

The Weidmüller Switch Configuration Utility window will open, as shown below.



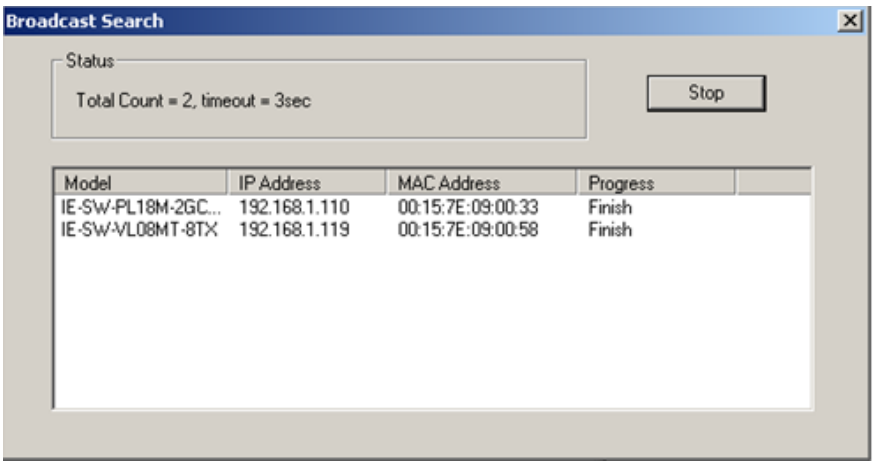
NOTE: You may download the Weidmüller Switch Configuration Utility free of charge from the Weidmüller Internet Server.

The information how to download is described in **Appendix C**.

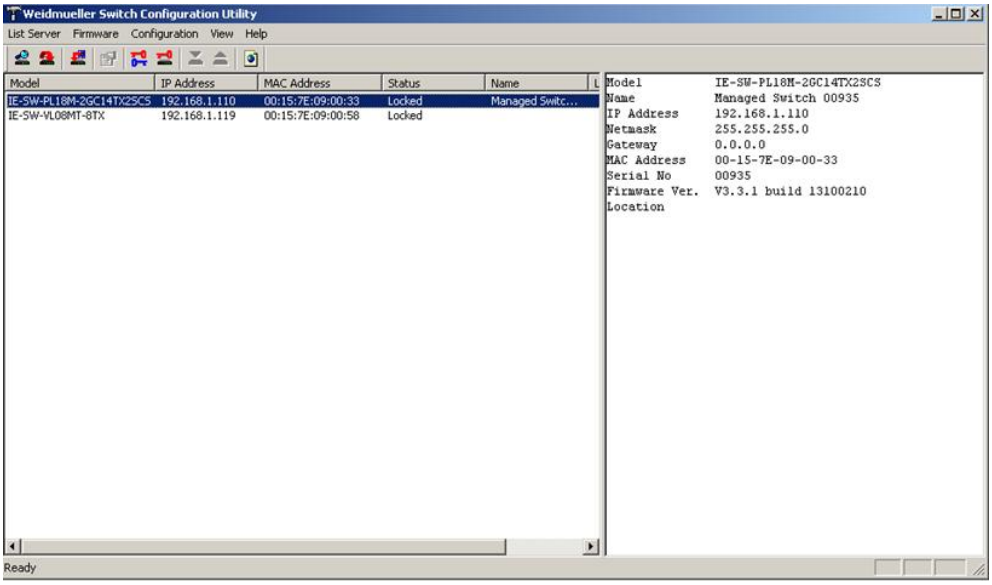
A1.2 Broadcast Search

Use the **Broadcast Search** function to search the LAN for all Weidmüller managed switches that are connected to the LAN. Note that since the search is done by MAC address, **Broadcast Search** will not be able to locate Weidmüller Ethernet Switches connected outside the PC host's LAN.

Start by clicking the Broadcast Search icon , or by selecting **Broadcast Search** under the **List Server** menu.The Broadcast Search window will open, displaying a list of all Weidmüller managed switches located on the network, as well as the progress of the search.



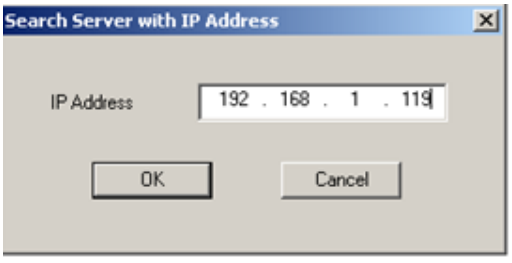
Once the search is complete, the Utility window will display a list of all switches that were located.



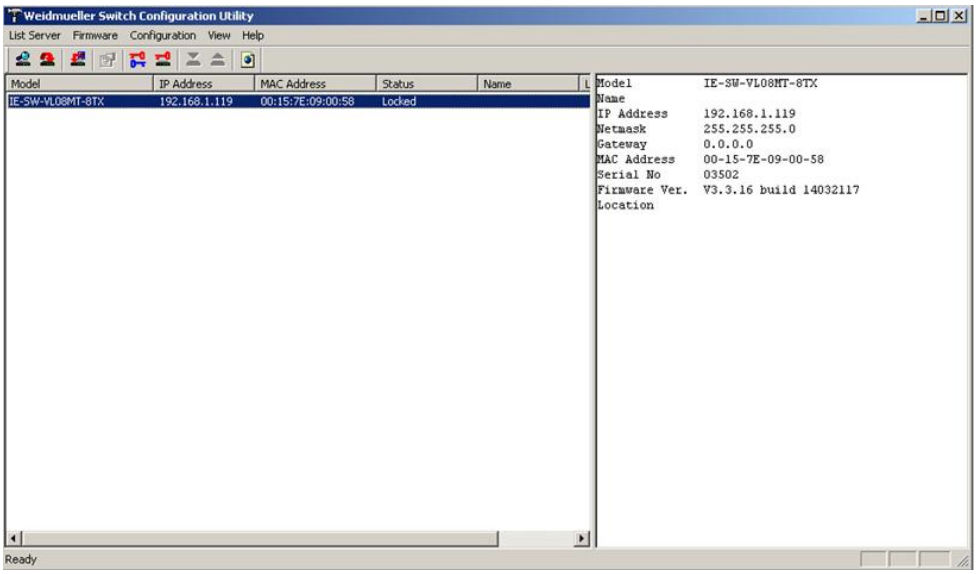
A1.3 Search by IP Address

Use the **Search by IP Address** function to search for Weidmüller managed switches one at a time. Note that the search is conducted by IP address, so you should be able to locate any Weidmüller switch that is properly connected to your LAN, WAN, or the Internet. Start by clicking the Specify by IP address icon , or by selecting **Specify IP address** under the **List Server** menu.

The **Search Server with IP Address** window will open. Enter the IP address of the switch you wish to search for, and then click **OK**.



Once the search is complete, the Utility window will add the switch to the list of switches.

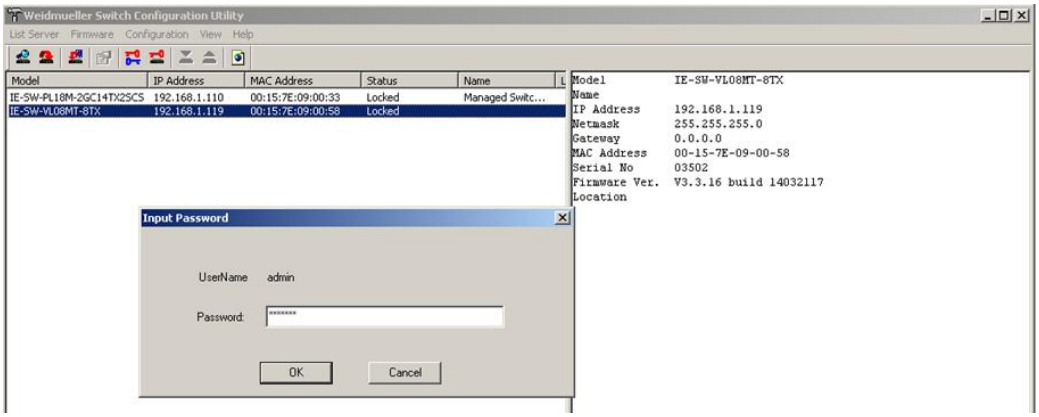


A1.4 Unlock the Ethernet Switch

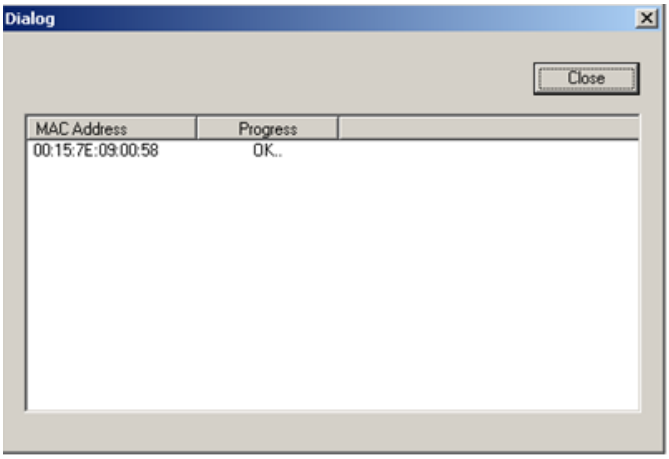
The **Unlock** function is used to open a password protected switch so that the user can modify its configuration, import/export a configuration and perform other procedures.

Follow the steps given below to unlock a locked Weidmüller switch. Highlight the switch (from the Ethernet Switch list in the Utility window's left pane), and then click the **Unlock** toolbar icon , or select **Unlock** from the **Configuration** menu.

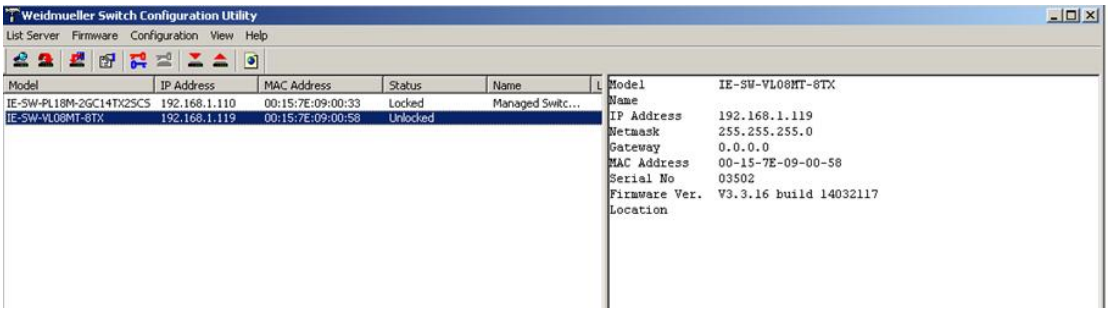
1. Enter the switch's **Password** when prompted, and then click **OK**.



2. When the **Dialog** window reports Progress as **OK**, click the **Close** button in the upper right corner of the window.



3. The status of the switch will now read **Unlocked**.



A1.5 Upgrade Firmware

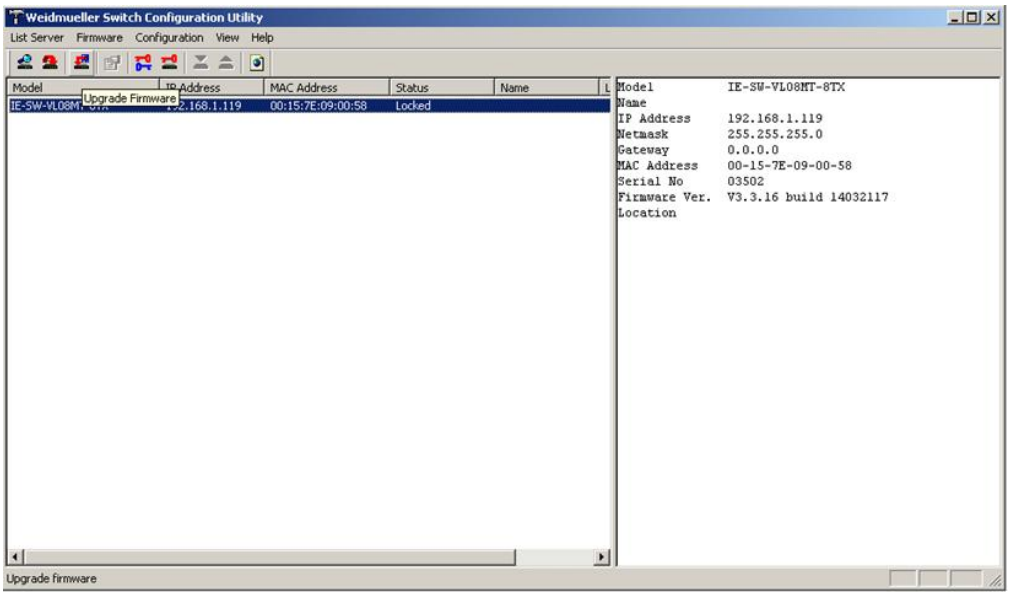
You may download the latest Firmware from the Weidmüller Internet Server.

The information how to download is described in **Appendix C**.

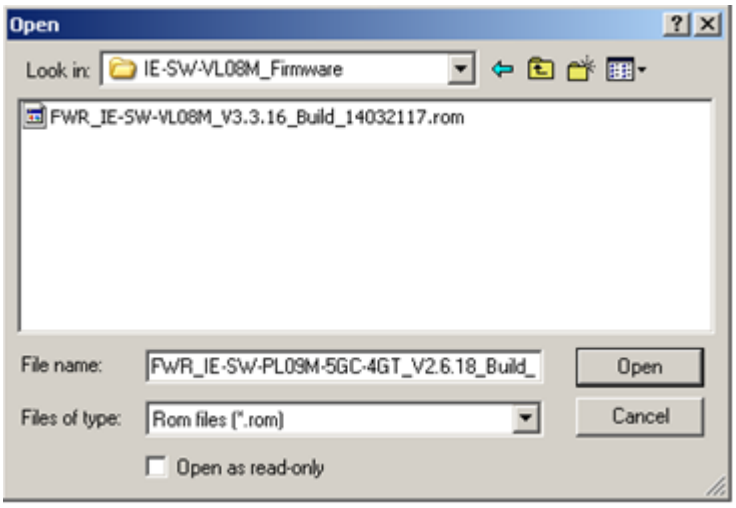
Keep your Weidmüller switch up to date with the latest firmware from Weidmüller. Perform the following steps to upgrade the firmware:

1. Download the firmware (*.rom) file from the Weidmüller website (www.weidmueller.com).

2. Click the switch (from the **Weidmüller Switch Configuration Utility** window) whose firmware you wish to upgrade to highlight it.



3. Click the **Upgrade Firmware** toolbar icon , or select **Upgrade** under the **Firmware** menu. The Switch has to be unlocked to be able to use this function. Use the **Open** window to navigate to the folder that contains the firmware upgrade file, and then click the correct "*.rom" file (**FWR_IE-SW-VL08M_V3.3.16_Build_14032117.rom** in the example shown below) to select the file. Click **Open** to activate the upgrade process.



A1.6 Modify IP Address

You may use the **Modify IP Address** function to reconfigure the Weidmüller switch network settings.

Start by clicking the Modify IP address icon , or by selecting **Modify IP address** under the **Configuration** menu. The Switch has to be unlocked to be able to use this function.

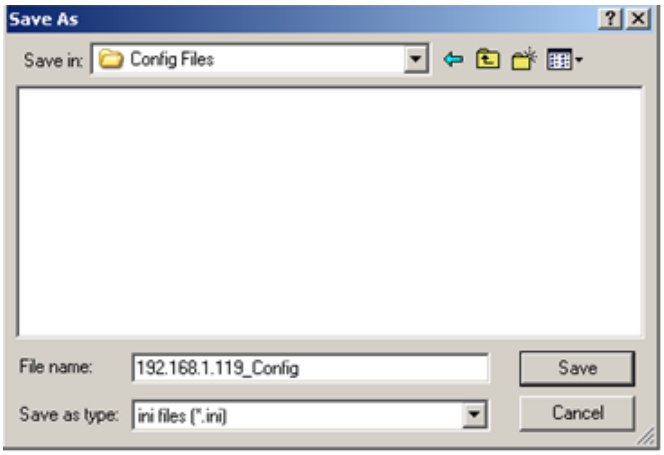
The **Setup Configuration** window will open. Checkmark the box to the left of those items that you wish to modify, and then Disable or Enable DHCP, and enter IP Address, Subnet mask, Gateway, and DNS IP. Click **OK** to accept the changes to the configuration.

Modify IP Address
Model Name: IE-SW-VL08MT-8TX
MAC address 00:15:7E:09:00:58
Serial Number 03502
AUTOIP
Disable
DHCP
Bootp
IP Address 192 . 168 . 1 . 119
Netmask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
DNS IP 0 . 0 . 0 . 0
DNS 2 IP 0 . 0 . 0 . 0
Tip: Click the check box to select/un-select change item.
OK
Cancel

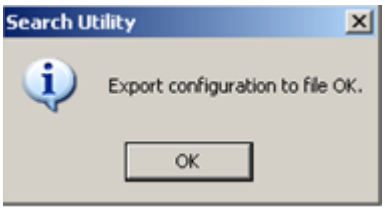
A1.7 Export Configuration

The **Export Configuration** function is used to save the entire configuration of a particular Weidmüller managed switch to a text file. The Switch has to be unlocked to be able to use this function.Take the following steps to export a configuration:

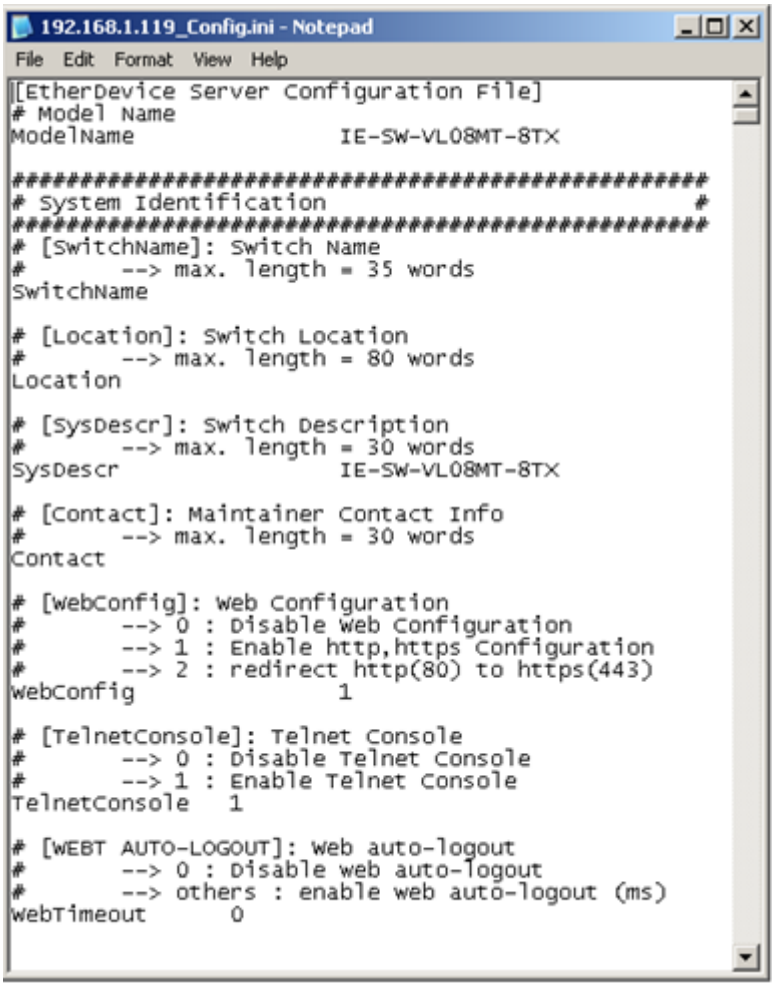
1. Highlight the switch (from the Server list in the Utility window's left pane), and then click the **Export** toolbar icon or select **Export Configuration** from the **Configuration** menu. Use the **Open** window to navigate to the folder in which you want to store the configuration, and then type the name of the file in the File name input box. Click **Save**.



1. Click **OK** when the **Export configuration to file OK** message appears.



2. You may use a standard text editor, such as Notepad under Windows, to view and modify the newly created configuration file.

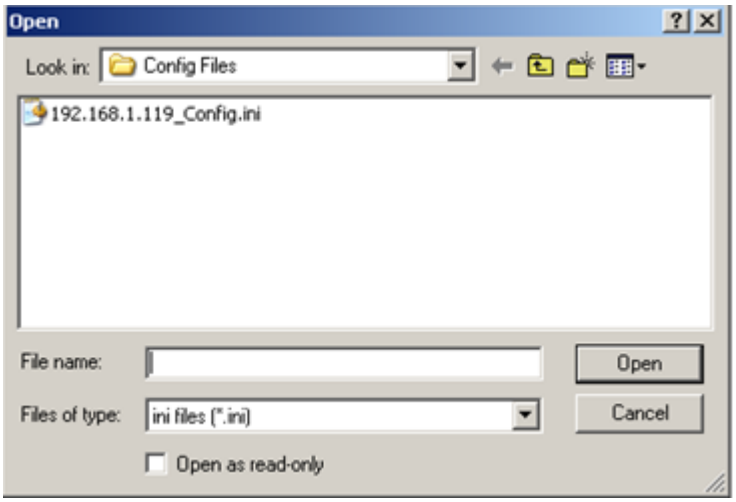

192.168.1.119_Config.ini - Notepad
File Edit Format View Help
[EtherDevice Server Configuration File]
Model Name
ModelName IE-SW-VL08MT-8TX
##
System Identification
##
[SwitchName]: Switch Name
--> max. length = 35 words
SwitchName
[Location]: Switch Location
--> max. length = 80 words
Location
[SysDescr]: Switch Description
--> max. length = 30 words
SysDescr IE-SW-VL08MT-8TX
[Contact]: Maintainer Contact Info
--> max. length = 30 words
Contact
[WebConfig]: Web Configuration
--> 0 : Disable Web Configuration
--> 1 : Enable http,https Configuration
--> 2 : redirect http(80) to https(443)
WebConfig 1
[TelnetConsole]: Telnet Console
--> 0 : Disable Telnet Console
--> 1 : Enable Telnet Console
TelnetConsole 1
[WEBT AUTO-LOGOUT]: Web auto-logout
--> 0 : Disable web auto-logout
--> others : enable web auto-logout (ms)
WebTimeout 0

A1.8 Import Configuration

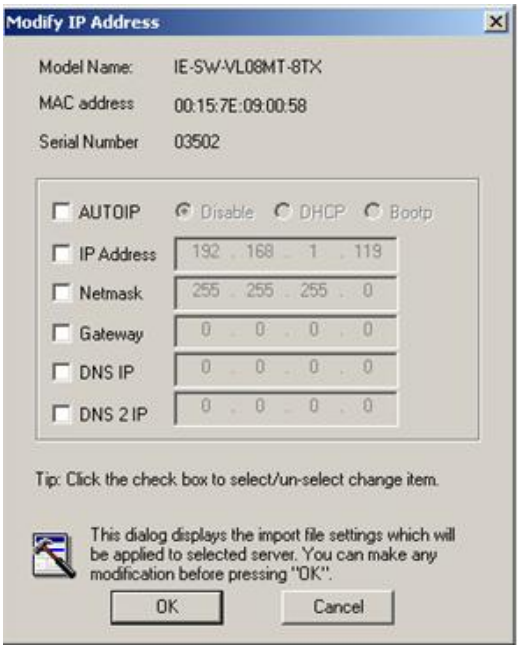
The **Import Configuration** function is used to import an entire configuration from a text file to the Weidmüller switch. The Switch has to be unlocked to be able to use this function.This function can be used to transfer the configuration from one Weidmüller managed switch to another, by first using the Export Configuration function (described in the previous section) to save a switch configuration to a file, and then using the Import Configuration function. Perform the following steps to import a configuration:

1. Highlight the switch (from the Ethernet Switch list in the Utility window's left pane), and then click the **Import** toolbar icon , or select **Import Configuration** from the **Configuration** menu.

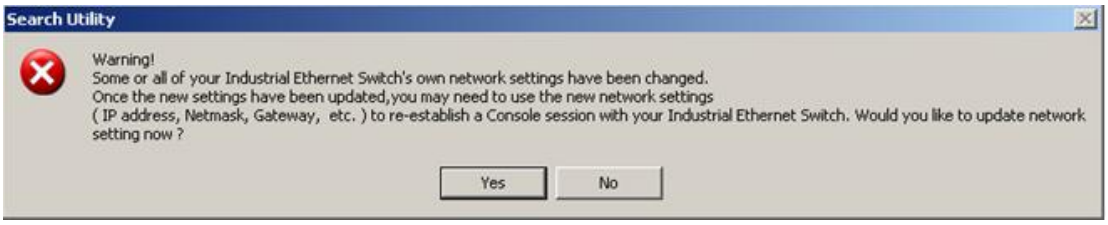
2. Use the **Open** window to navigate to the text file that contains the desired configuration. Once the file is selected, click **Open** to initiate the import procedure.



3. The **Setup Configuration** window will be displayed, with a special note attached at the bottom. Parameters that have been changed will be activated with a checkmark. You may make more changes if necessary, and then click **OK** to accept the changes.



4. Click **Yes** in response to the following warning message to accept the new settings.


Search Utility
Warning!
Some or all of your Industrial Ethernet Switch's own network settings have been changed.
Once the new settings have been updated,you may need to use the new network settings
(IP address, Netmask, Gateway, etc.) to re-establish a Console session with your Industrial Ethernet Switch. Would you like to update network setting now ?
Yes
No

B. MIB Groups

B1.1 Supported standard MIB II groups

The Weidmüller switch comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold/warm start trap, line up/down trap, and RFC 1213 MIB-II.

The standard MIB groups supported by the Weidmüller switch are:

MIB II.1 – System Group
- sysORTable

MIB II.2 – Interfaces Group
- ifTable

MIB II.4 – IP Group
- ipAddrTable
- ipNetToMediaTable
- IpGroup
- IpBasicStatsGroup
- IpStatsGroup

MIB II.5 – ICMP Group
- IcmpGroup
- IcmpInputStatus
- IcmpOutputStats

MIB II.6 – TCP Group
- tcpConnTable
- TcpGroup
- TcpStats

MIB II.7 – UDP Group
- udpTable
- UdpStats

MIB II.10 – Transmission Group
- dot3
- dot3StatsTable

MIB II.11 – SNMP Group
- SnmpBasicGroup
- SnmpInputStats
- SnmpOutputStats

MIB II.17 – dot1dBridge Group
- dot1dBase
  - dot1dBasePortTable
- dot1dStp
  - dot1dStpPortTable
- dot1dTp
  - dot1dTpFdbTable
  - dot1dTpPortTable
  - dot1dTpHCPortTable
  - dot1dTpPortOverflowTable
- pBridgeMIB
  - dot1dExtBase
  - dot1dPriority

dot1dGarp
qBridgeMIB
dot1qBase
dot1qTp
dot1qFdbTable
dot1qTpPortTable
dot1qTpGroupTable
dot1qForwardUnregisteredTable
dot1qStatic
dot1qStaticUnicastTable
dot1qStaticMulticastTable
dot1qVlan
dot1qVlanCurrentTable
dot1qVlanStaticTable
dot1qPortVlanTable

Additionally for each Weidmüller managed switch series a private MIB file is available which can be downloaded from the Weidmüller Internet Server (Download information described in **Appendix C**).

B1.2 Implemented SNMP Traps

Public Traps:

- Cold Start
- Link Up
- Link Down
- Authentication Failure
- dot1dBridge New Root
- dot1dBridge Topology Changed

Private Traps:

- Configuration Changed
- Power On
- Power Off
- Traffic Overloaded
- Turbo Ring Topology Changed
- Turbo Ring Coupling Port Changed
- Turbo Ring Master Mismatch

C. Download links (Software and Documentation)

Using below described links you can download following items:

- Firmware Upgrades
- Private MIB files
- Profinet GSDML file
- Weidmüller Switch Configuration Utility
- Documentation (User Manual and Hardware Installation Guide)

Option 1: Download via **Product Catalogue (Online Catalogue)**

Download latest Firmware version, Private MIB file, Profinet GSDML file, Tool Switch Configuration Utility or Documentation.

http://www.weidmueller.com

► Select Product Catalogue
⇨ Select „Active Industrial Ethernet“
⇨ Select „Managed Switch‘ product group“ (eg. ValueLine managed Switches)
⇨ Select Product model
⇨ Click and expand section „Downloads“
⇨ Download the needed items

Option 2: Download via **Weidmüller Corporate Website (Download area)**

Download ZIP-file (containing latest Firmware version, Private MIB file, Profinet GSDML file) or Tool Switch Configuration Utility.

http://www.weidmueller.com

⇨ Select Downloads
⇨ Select **Software**
⇨ Select „Industrial Ethernet“
⇨ Goto section **Value and Premium Line managed Switches (Firmware, GSDML, SNMP MIB)**
⇨ Download *ZIP-file of the respective managed switch model*
⇨ Goto section **Value and Premium Line managed Switches (Software Tools)**
⇨ Download *Weidmüller Switch Configuration Utility (V 1.0)*

Download product documentation (User manual, Hardware Installation Guide) via Download section of Weidmüller Internet Server.

http://www.weidmueller.com

⇨ Select Downloads
⇨ Select **Print Media**
⇨ Select „Manuals“
⇨ Goto section „Industrial Ethernet“
⇨ Download PDF-file *Manual_Managed_Switches_WM…..pdf*
⇨ Select „Operating Instructions“
⇨ Goto section „Industrial Ethernet (Hardware Installation Guides)“
⇨ Download PDF-file *of the respective managed switch model.*